2022
6ª EDIZIONE

AFCEA
CAPITOLO DI ROMA

Un anno di attività

www.afcearoma.it

Care amiche e cari amici del Capitolo di Roma di AFCEA International,

siamo ormai giunti alla sesta edizione della nostra rivista che, con il Comitato di Redazione continuiamo a realizzare e migliorare, spinti anche dal vostro apprezzamento e gradimento.

Visto il favorevole accoglimento, anche quest'anno abbiamo deciso di riproporre la novità introdotta nella scorsa edizione: una sezione costituita da una raccolta di articoli su argomenti di interesse per AFCEA, redatti dai nostri soci Corporate sulla base delle proprie competenze; che è stata arricchita da due articoli redatti dalla sezione "Women in AFCEA". Tale sezione è ulteriormente valorizzata da due articoli esclusivi scritti per la nostra rivista, uno dal Presidente e CEO di AFCEA International, il Lt. Gen. Susan Lawrence, USA (Ret.) ed l'altro dal General Manager di AFCEA Europe, il Maj. Gen. Ercih Staudacher, GEAF (Ret.)

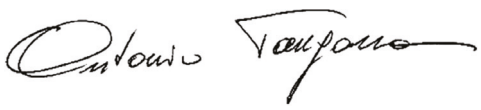
Grazie all'attenuarsi della pandemia Covid, lo scorso anno dopo un primo periodo in cui abbiamo organizzato eventi da remoto, dalla seconda metà di giugno abbiamo ripreso le attività in presenza; di tutti i convegni potete trovare la sintesi nella sezione "Eventi". Colgo l'occasione per ringraziare ulteriormente tutti i relatori che, provenienti da settori diversi, istituzionale, accademico e industriale, hanno sempre valorizzato al meglio le tematiche affrontate nei singoli convegni.

Le difficoltà del periodo pandemico avevano stimolato anche attività migliorative e quindi abbiamo mantenuto viva, grazie al supporto di alcuni soci, la pubblicazione sul sito e la segnalazione via mail di articoli, report, documenti tecnici e notifiche di webinar organizzati dalle aziende Socie e da AFCEA International sui temi di rilevanza e attualità nei campi d'interesse dell'Associazione.

In definitiva tutte queste attività sono orientate al perseguimento del principale obiettivo di AFCEA, vale a dire la promozione del il dialogo tra comunità militari, governative, accademiche e industriali per ampliare la cultura e le conoscenze professionali nei settori delle comunicazioni, del comando e controllo, dell'Information Technology, dell'intelligence, della sicurezza e dello spazio. Anche quest'anno, in conclusione mi piace ricordare e sottolineare che il Capitolo di Roma di AFCEA International è un'associazione no profit costituita da soci che operano su base esclusivamente volontaria con impegno e passione ed esprimere un sentito ringraziamento a coloro che, operando quotidianamente anche al di là dei propri impegni personali e lavorativi, assicurano l'operatività di uno dei maggiori Capitoli dell'Associazione, consentendogli di ottenere numerosi e importanti riconoscimenti da parte di AFCEA International.

Nell'invitarvi a seguirci sempre sul nostro sito e a partecipare ai nostri eventi, rivolgo a tutti l'augurio di una piacevole lettura con un arrivederci alla prossima edizione.

IL PRESIDENTE
Gen.Isp.Capo (r) Antonio ing. TANGORRA



Indice dei contenuti

AFCEA Capitolo di Roma

AFCEA International è un'associazione no profit il cui principale obiettivo è promuovere il dialogo tra comunità militari, governative, accademiche e industriali per ampliare la cultura e le conoscenze professionali nei settori delle comunicazioni, del comando e controllo, dell'Information Technology, dell'intelligence, della sicurezza e dello spazio.
Costituita negli Stati Uniti nel 1946 dopo la seconda guerra mondiale per raggruppare i veterani dei "battaglioni SIGNAL", AFCEA International cominciò a includere già nello stesso anno la componente industriale. A partire dal 1979 ha avuto inizio il processo di internazionalizzazione che ha portato alla creazione di Capitoli locali in Canada, Sud America, Europa, Asia, Australia, oltre che negli Stati Uniti per un totale di 138 capitoli in 33 Paesi.
Attraverso i suoi Capitoli, AFCEA International può contare attualmente su oltre 26.000 soci individuali e circa 1.600 soci corporate, costituendo così un vastissimo network i cui valori chiave sono l'etica, la professionalità, l'impegno, la qualità, la formazione e il rispetto delle diversità. Questo ampio network internazionale consente alle comunità coinvolte di cooperare per allineare tecnologie e strategie innovative ai requisiti sempre più sfidanti di coloro che servono le istituzioni. Ogni Capitolo ha una propria organizzazione e svolge le proprie attività in autonomia, in coordinamento con la comunità di AFCEA International e in linea con i suoi principi fondamentali.

Il **Capitolo di Roma** fu costituito nel 1988 e da allora rappresenta un costante e qualificato riferimento per i principali operatori a livello nazionale nei settori dell'Information Technology, Comunicazioni, Difesa, Sicurezza e Spazio, grazie alla capacità di raccogliere e armonizzare contributi provenienti dalle istituzioni, dagli enti di ricerca e università, dalle grandi industrie nonché dalle piccole e medie imprese.

AFCEA International ogni anno assegna numerosi riconoscimenti ai capitoli e ai soci che si sono particolarmente distinti con il loro impegno in riconoscimento delle attività svolte e dei risultati ottenuti. Nel 2021 il nostro Capitolo è stato premiato con il *Model Chapter Award*, il Dott. Marco Braccioli con il *Meritorious Service Award*.
Il Capitolo partecipa attivamente alla vita di AFCEA International: il Presidente Gen.Isp.Capo(r) Antonio Tangorra è membro del Board of Directors di AFCEA International, inoltre è stato nominato Vice President per la Regione Mediterranea; la Dott.ssa Fiorella Lamberti è anch'essa membro del Board of Directors nonché rappresentante del Capitolo in "Women in AFCEA" Subcommittee; l'Avv. Alessandra Finocchio e l'Ing. Vincenzo Vitiello sono membri dell'AFCEA International Membership Committee che ha lo scopo di promuovere la crescita del valore dell'appartenenza ad AFCEA, il Dott. Stefano Tangorra è il rappresentante in Young AFCEAn in Europe.

L'organizzazione

Il Capitolo è un'organizzazione molto dinamica e fluida con un continuo ricambio intorno ad un nucleo consolidato e storico; lo scorso anno AFCEA International ha conferito dei riconoscimenti ai soci con affiliazione di 15, 25, 30 e 40 anni. Ad oggi il Capitolo di Roma può contare su oltre 400 soci individuali e 40 corporate. Tutti i soci iscritti al Capitolo formano l'Assemblea che elegge il Presidente, i due Vice Presidenti, il Consiglio Direttivo il Comitato Tecnico Scientifico e i Proboviri.

Il vertice è costituito dal Presidente e due Vice Presidenti eletti annualmente e provenienti singolarmente dai settori rappresentativi dell'Associazione: militare, industriale, accademico. Completano il quadro degli Organi dell'Associazione il Segretario e il Tesoriere, designati dal Presidente, e tre Probiviri, eletti ogni tre anni. Il Consiglio Direttivo, costituito da 15 membri eletti annualmente, definisce ed approva le differenti iniziative, il programma delle attività e le spese relative. Il Comitato Tecnico Scientifico, costituito da 5 membri eletti annualmente, ha il compito di assicurare che le attività dell'Associazione propongano contenuti tecnico-scientifici adeguati ed innovativi, attraverso la selezione di argomenti e tematiche che possano stimolare una divulgazione puntuale ed uno scambio culturale tra tutti partecipanti alla vita dell'Associazione.

Inoltre, è attivo il Comitato di Redazione, che ha la responsabilità di tutte le attività Editoriali e di Comunicazione tra cui quelle svolte tramite il sito web.

In linea con le corrispondenti commissioni già istituite da AFCEA International, il Capitolo di Roma ha creato al proprio interno due sezioni dedicate, AFCEA Youth e Women in AFCEA:

- **AFCEA Youth** ha lo scopo di coinvolgere giovani studenti nella vita dell'associazione, anche attraverso la costituzione di Student Club dedicati, per avvicinarli sempre di più al mondo del business nei settori della difesa e della sicurezza, invitandoli a sostenere gli obiettivi tecnico-scientifici dell'associazione con i loro progetti.
- **Women in AFCEA Rome Chapter** è nata per sostenere e valorizzare la presenza delle donne nel mondo istituzionale, accademico e industriale nei settori di interesse dell'Associazione con particolare attenzione all'ambito STEM (Science, Technology, Engineering and Mathematics).

Le attività

L'appartenenza al Capitolo di Roma fornisce l'accesso ad una vasta e qualificata platea per i professionisti del settore pubblico e privato nelle aree delle Comunicazioni, della Cyber, dei Sistemi Informatici, Elettronici e di Comando e Controllo nell'ambito della Difesa, della Sicurezza e dell'Industria che opera in tali settori.

A tal fine ogni anno il Capitolo definisce il proprio programma di attività con il contributo dei soci per organizzare riunioni, seminari, conferenze, visite o altre iniziative per mantenere i suoi membri aggiornati sulle problematiche nei settori d'interesse. L'accesso ai seminari e conferenze è libero per tutti gli interessati. La comunicazione degli eventi avviene tramite il sito dell'Associazione e Linkedin. Il calendario degli eventi è pubblicato anche sul sito di AFCEA International.
A questa vengono poi inviati i report di ogni evento per la pubblicazione su SIGNAL, rivista ufficiale dell'Associazione, offrendo così anche l'opportunità di presentarsi a una vetrina internazionale.

In particolare le principali attività sono articolate in:

- **Convegni:** sulla base delle principali tematiche scelte ogni anno dal Consiglio Direttivo con il supporto del Comitato Tecnico Scientifico, i convegni hanno l'obiettivo di fare il punto su argomenti di particolare interesse ed attualità attraverso la partecipazione delle principali istituzioni coinvolte, del mondo accademico e dell'industrie che operano nei settori di riferimento.

- **Presentazioni aziendali:** ogni socio "corporate" ha la possibilità di effettuare una presentazione su un argomento specifico, giudicato d'interesse dal Consiglio Direttivo con il supporto del Comitato Tecnico Scientifico, per illustrare le problematiche connesse e le proprie proposte e soluzioni, anche utilizzando "case study" con istituzioni e/o mondo accademico.

- **Visite:** AFCEA organizza per i propri soci una serie di visite presso strutture istituzionali, come pure siti d'interesse dal punto di vista culturale e scientifico per incoraggiare la disseminazione della conoscenza tecnologica e della cultura tra i propri membri, sia in ambiti prettamente legati alla Difesa e alla Sicurezza sia in ambiti di carattere culturale più generale.

- **Master:** Il Capitolo di Roma sostiene le attività di formazione finanziando da molti anni tre borse per due Master di II livello in: "Ingegneria e Diritto Internazionale dello Spazio nei Sistemi di Comunicazione, Navigazione e Sensing Satellitare" dell'Università di Roma Tor Vergata e in "Optics and Quantum Information" presso l'Università di Roma La Sapienza.

L'Associazione ha stipulato convenzioni con altri Enti e liberi professionisti per fornire opportunità e facilitazioni ai Soci.

Il sito

Tutte le informazioni sulla storia del Capitolo di Roma, la sua organizzazione, le sue attività, le modalità di associazione, i soci "Corporate" con i rispettivi loghi e profili sono disponibili sul sito web www.afcearoma.it.
In particolare il sito, per ogni evento organizzato, mette a disposizione le presentazioni e le riprese effettuate, nonché un report con una sintesi degli interventi dei vari relatori. In questo modo tutti i soci e i visitatori del sito interessati hanno la possibilità di mantenersi aggiornati e conoscere i contenuti dettagliati.
Tutti i soci hanno anche la possibilità di fare conoscere le proprie attività professionali attraverso la pubblicazione di articoli di elevato contenuto professionale e di notizie di rilevante interesse.
Sono inoltre disponibili informazioni sugli accordi e convenzioni stipulati con altre Associazioni e Organizzazioni.

Gli eventi 2021

GLI SCENARI SIMULATIVI PER LE COMUNICAZIONI RADIO NEL CONTESTO OPERATIVO MILITARE

Webinar, 16 marzo 2021

AFCEA Capitolo di Roma e il socio CRISEL hanno organizzato questo webinar, con il supporto della società SPIRENT, per discutere i potenziali scenari critici nelle comunicazioni radio e la pianificazione di un'efficace simulazione, in modo da verificare la robustezza delle trasmissioni nei diversi ambiti operativi e tattici.

In particolare, durante il webinar è stato spiegato perché i test di laboratorio, in grado di ricreare fedelmente gli scenari operativi, offrono maggiori possibilità rispetto ai test sul campo, illustrando i vantaggi che l'operatore può ottenere utilizzando piattaforme automatizzate di test.

Nel corso del webinar sono state poi illustrate le configurazioni nei casi di test su radio di tipo MESH, satellitare e privata, evidenziando gli aspetti da considerare nei sistemi di comunicazione "Mission-Critical" quando si definiscono le procedure di test di sistema. Sono stati infine presentati alcuni casi reali di studio per meglio illustrare l'esperienza e il know-how di SPIRENT Communications in questo settore di applicazione.

Dott. Francesco P. Pacillo - Crisel - Chi è Crisel

Dott. Francesco P. Pacillo - Crisel - Chi è Spirent Communications

Mr.Jukka-Pukka Nuutinen, Senior Solutions Architect - Spirent - What is Vertex and what does it do?

Mr.Jukka-Pukka Nuutinen, Senior Solutions Architect - Spirent - Vertex in military applications: MESH radios, Private radios, Satellite radios

Mr.Jukka-Pukka Nuutinen, Senior Solutions Architect - Spirent - How to get the best out of Vertex : Designing a systematic test strategy

Mr Frederic Touma, EMEA Wireless Business Development Manager Case studies & examples

Mr.Jukka-Pukka Nuutinen, Senior Solutions Architect - Spirent - Closing remarks

L'INTELLIGENZA ARTIFICIALE APPLICATA IN AMBITO MILITARE: PROSPETTIVE E POSSIBILI CASI D'USO

Webinar, 25 marzo 2021

L'Intelligenza Artificiale o Artificial Intelligence (AI) – che comprende una serie di tecnologie come "machine learning" e "natural language processing" - consente alle macchine di percepire, comprendere, agire e apprendere, con l'obiettivo di aumentare le potenzialità umane. Si tratta di una delle cosiddette "Emerging Disruptive Technologies" che sta cominciando a diffondersi in modo pervasivo in molti settori della nostra società. Ovviamente tale fenomeno ha un forte impatto anche nel contesto militare. Recenti studi prevedono che nei prossimi anni l'influenza dell'intelligenza artificiale per il settore aerospaziale e difesa sarà di gran lunga superiore a quello di qualunque altra tecnologia emergente.

Manutenzione Predittiva, Applicazioni Aeronautiche, Applicazioni di attacco e difesa digitale per il V Dominio, Supporto allo sviluppo dei sistemi complessi, Controllo dello stato di efficienza delle piste di decollo e atterraggio, Rilevamento e tracciamento velivoli, analisi di big data e applicazioni geospaziali, sono solo alcuni esempi di ambiti in cui sono in atto cambiamenti basati su tecniche di Intelligenza Artificiale.

In questo contesto AFCEA Capitolo di Roma ha organizzato questo webinair sull'Intelligenza Artificiale, per fornire una prima panoramica sul suo possibile impiego in ambito militare; una panoramica necessariamente limitata, successivamente ampliata con un altro incontro dedicato che ha avuto luogo il 24 giugno. Attraverso il webinar sono state presentate alcune esperienze sviluppate sia a livello istituzionale sia a livello industriale, con riferimento ai requisiti del settore. L'applicazione di questa tecnologia complessa deve comunque includere la presenza umana nel ciclo delle decisioni, per poter adottare con consapevolezza l'AI sfruttandone i benefici e riducendone i rischi.

Organizzato da AFCEA Capitolo di Roma con il supporto di ESRI Italia che ha messo a disposizione il proprio Theater di Via Casilina, Roma per la trasmissione, il webinar è stato moderato dal dott. Marco Braccioli, Vice President Defense & Cyber Security, Digital Platforms.

Dott. Domenico Natale – UNINFO - Le intelligenze artificiali
Ing. Alessandro Capucci – ASC27 - AI Cognitiva. Emulazione, Riconoscimento ed Empatia: Minacce e Opportunità per Difensori e Attaccanti
Prof. Dott. Stefano Bellucci - RAIT88 - L'intelligenza artificiale nell'apprendimento autonomo e nell'integrazione coi sistemi C2
Ing. Alessandro Marchini – EURELETTRONICAICAS - Mobile GRF Runway Inspector
Col. Giacomo Ghiglierio - RESIA - Comando Logistico A.M. - Digital Innovation Hangar - l'approccio dell'Aeronautica Militare alle tecnologie innovative
Dott. Antonio Cerqua – ALMAVIVA - Intelligenza Artificiale applicata alla manutenzione predittiva in ambito trasporti e assetti mobili
Dott. Giorgio Forti - ESRI ITALIA - Deep Learning e Big Data Analytics in ambito geospaziale: l'esperienza di Esri Italia

L'IMPORTANZA DELLA VIRTUALIZZAZIONE E POSSIBILI SOLUZIONI OPEN SOURCE

Webinar, 4 giugno 2021

AFCEA Capitolo di Roma e l'associata società francese VATES Sas hanno organizzato un webinair sulla virtualizzazione con particolare riferimento alle soluzioni open source. Le tecnologie di virtualizzazione sono il cuore degli attuali data center, dell'hybrid cloud e anche dei campi di battaglia informatici. Pertanto, sono componenti critici della gestione dell'infrastruttura IT e della sicurezza informatica. La virtualizzazione inoltre aiuta a ridurre i costi e a far sì che l'infrastruttura disponibile sia più efficace e produttiva.

Vates è uno dei pochi attori esclusivamente europeo nello sviluppo chiavi in mano di soluzioni per la gestione delle infrastrutture più diverse, open source e sicure. I suoi punti di forza sono l'innovazione, la qualità del supporto clienti senza compromessi, le soluzioni chiavi in mano e sicure.
Vates collabora inoltre con differenti istituzioni accademiche in Francia per lavorare a stretto contatto con i ricercatori e portare l'innovazione dal campo della ricerca alla piattaforma XCR-ng.

Nel corso del webinar il management della società ha illustrato i prodotti XCP-ng e Xen Orchestra, introducendo poi dei partner e degli interessanti uses cases.

Mr Marc Pezin, Chief Marketing Director – VATES - Presentation of Vates ,
Mr Olivier Lambert, CEO - VATES - The importance of virtualization
Mr Olivier Lambert, CEO – VATES - Introduction to Xen Orchestra
Mr Olivier Lambert, CEO – VATES - Introduction to XCP-ng
Mr Olivier Lambert, CEO – VATES - VmWare & Citrix: how Vates can help you
Mr Stany Wyrzykowski, CEO - C2D System House - Customer use case
2CRSi Marketing Director: Partner spotlight
Mr Charles - H. Schulz, CSO - VATES - Cybersecurity and edge use cases

L'INTELLIGENZA ARTIFICIALE APPLICATA IN AMBITO MILITARE: PROSPETTIVE E POSSIBILI CASI D'USO - SECONDO ROUND

Webinar, 24 giugno 2021

Dopo il primo appuntamento del 25 marzo 2021, sull'Intelligenza Artificiale dedicato in particolare all'Aeronautica, il Capitolo di Roma di AFCEA International ha deciso di continuare il suo viaggio nel mondo dell'Intelligenza Artificiale con uno sguardo particolare al settore Militare, esplorando le applicazioni e i possibili casi d'uso che riguardano Esercito e Marina.

L'Intelligenza Artificiale o Artificial Intelligence (AI) – che comprende una serie di tecnologie come "machine learning" e "natural language processing" - consente alle macchine di percepire, comprendere, agire e apprendere, con l'obiettivo di aumentare le potenzialità umane. Si tratta di una delle cosiddette "Emerging Disruptive Technologies" che sta cominciando a diffondersi in modo pervasivo in molti settori della nostra società. Ovviamente tale fenomeno ha un forte impatto anche nel contesto militare. Recenti studi prevedono che nei prossimi anni l'influenza dell'intelligenza artificiale per il settore aerospaziale e difesa sarà di gran lunga superiore a quello di qualunque altra tecnologia emergente. La stessa Nato ha promosso un Advisory Group di esperti per valutare l'impatto dell'AI nel confronto futuro con i blocchi avversari.

Questa complessa tecnologia tipicamente "dual use" deve comunque includere la presenza umana nel ciclo delle decisioni, per poter adottare con consapevolezza l'AI e sfruttarne i benefici, riducendone i rischi.

In questo contesto AFCEA Capitolo di Roma ha pertanto deciso di approfondire questi aspetti con un secondo webinar sull'A.I. per fornire una ulteriore panoramica sul suo possibile impiego in ambito militare con particolare riferimento a Esercito e Marina. All'evento hanno partecipato anche istituzioni accademiche e industrie, le cui attività possono avere ricadute nel mondo militare in modo diretto e indiretto.

Ing. Marco Massenzi - TELECONSYS - RenAIssance – Lo sviluppo dell'Artificial Intelligence per un nuovo Rinascimento digitale: come adottarla nella propria organizzazione

Ing. Alessandro Massa – LEONARDO - L'intelligenza artificiale nelle applicazioni militari. Casi d'uso, e ambiti di ricerca

Ing. Daniele Babbanini - VITROCISET - L'utilizzo dell'Intelligenza artificiale a bordo di Sistemi Unmanned,

C. V. Giuseppe Rizzi - STATO MAGGIORE MARINA - Intelligenza Artificiale negli attuali e futuri sistemi della Marina Militare

Magg. Daniele Paniconi - STATO MAGGIORE ESERCITO - Artificial Intelligence e autonomia nell'ambito della campagna di sperimentazione sui Robotic and Autonomous Systems (RAS) avviata dall'Esercito Italiano

Dott. Marco Taurone/Dott. Giancluca Zaccagnino - ASCITAL – Intelligenza Artioficiale al servizio di tecnologia, innovazione e ingegneria

Dott.ssa Sara Zollini - UNIVERSITA' DELL'AQUILA - Intelligenza Artificiale e tecniche geomatiche per la prevenzione del territorio

5G ECOSYSTEM E CYBER-SECURITY NEI CONTESTI CIVILI E MILITARI

7 ottobre 2021

Nel corso del seminario, primo evento in presenza dall'inizio della pandemia di Covid-19 del febbraio 2020, sono stati trattati i temi innovativi di maggior interesse connessi alla tecnologia 5G, la nuova generazione di comunicazioni mobili che offre potenzialità finora inespresse in ambito applicativo civile e militare (ad esempio, scaricamento di grossi contenuti e video alta definizione, realtà virtuale, veicoli autonomi, chirurgia a distanza e le reti di sensori IoT) e che rende gli attuali sistemi di comunicazione estremamente più efficienti, in termini sia di banda e velocità delle connessioni, sia di qualità dei servizi, affidabilità, continuità e sicurezza più in generale.

Alle reti 5G in via di realizzazione si integra l'aumento dei dispositivi IoT nelle reti di comunicazione e nelle infrastrutture critiche, così come negli ambiti applicativi sia civili sia militari; basti citare, nel contesto militare, la possibilità di utilizzare i dispositivi IOBT (Internet of the Battlfield Things) anche in teatro operativo, ad esempio per monitorare le condizioni fisiche dei soldati tramite dei sensori incorporati nelle divise militari o nei giubbetti antiproiettile.

L'aumento pervasivo dei dispostivi 5G ha però fatto lievitare i rischi di attacchi informatici di vario genere, poiché gli accessi e connessioni ai dispositivi IoT/5G non sono tutti conformi agli standard minimi di sicurezza e quindi rappresentano possibili punti di accesso e attacco cyber alla rete stessa. Il seminario è stata dunque un'occasione per fornire un'ampia panoramica sul tema, in ambito sia civile sia militare, in un contesto integrato di cyber security con nuove tecniche di autenticazione e crittografia.
Nel corso dell'evento, inoltre, il Magg. Gen(r) Erich Staudacher, General Manager di AFCEA Europa, ha consegnato un riconoscimento da parte di AFCEA international ai soci del Capitolo di Roma di più lunga appartenenza.

Prof. Nicola BLEFARI MELAZZI – Università di Tor Vergata – "5G e sicurezza delle reti"
Col. Marco PALLONE – Stato Maggiore Difesa VI° Reparto – "L'implementazione delle tecnologie 5G in ambito Difesa: vision strategica"
Ing. Guido BOTTALE – Leonardo SpA – "5G per la Difesa: Opportunità e sfide"
Dir. Luca SALAMONE – Segredifesa V° Reparto – "La cyber ed il 5G nell'ambito del Piano Nazionale di Ricerca Militare"
Col. Valerio GOLINO – Stato Maggiore Esercito VI° Reparto – "Possibili applicazioni militari terrestri della tecnologia 5G"
Dott. Stefano DELLA VALLE – Teleconsys – "A trusted IOT Platform over 5G"
Dott. Simone SANTI – Fortinet – "Strategie ZTNA e soluzioni SASE in risposta alle moderne sfide per la sicurezza"
Dott. Marco BRACCIOLI – Digital Platform – "5G, IoT, SMART GRID e IoBT"

DALL'IMAGE EXPLOITATION ALLA SITUATIONAL AWARENESS: SOLUZIONI GEOSPAZIALI PER LA DIFESA

17 novembre 2021

In un mondo in cui gli scenari militari sono sempre più complessi e tecnologici, in cui la crescita dei dati prodotti da ogni singolo sistema è in costante aumento mentre l'intelligenza artificiale viene applicata in ogni attività, diventa fondamentale padroneggiare strumenti avanzati di processamento di dati e di Situational Awareness per difendersi dalle minacce esterne ed avere la supremazia tecnologica al fine di sfruttare a proprio favore queste sfide.

Hexagon, organizzatrice dell'evento con il supporto di AFCEA – Capitolo di Roma, nel corso del Convegno ha illustrato il suo valore aggiunto nell'innovazione tecnologica, in particolare con le Geo-Ops solutions realizzate per rispondere alle principali sfide nel settore della Difesa, e nel dare la possibilità a stati, organizzazioni governative e integratori di sistema di aumentare la propria produttività e di avere a disposizione capacità per fronteggiare le minacce del domani.

Attraverso la divisione Geospatial di Hexagon affronta e risolve alcune tra le criticità più difficili che la società di oggi pone, rispondendo ai bisogni del mercato geospaziale in maniera veloce ed innovativa.

Filippo TROIANI – Hexagon's Geospatial Division – "Dai Sensori alla Real-Time Situational Awareness: le soluzioni complete di Hexagon"
Tom CRAUWELS – Hexagon's Geospatial Division – "Dimostrazione tecnica della piattaforma Luciad"
Dino QUATTROCIOCCHI – e-Geos – "Soluzioni e-Geos per la Difesa e l'Intelligence"
Giovanni FUMIA – Sky Eye Systems in collaborazione con Planetek Italia – "APR a lungo raggio e capacità ISR integrate"
Angelo GAZZONI – Hexagon's Safety & Infrastructure Division – "HxGN OnCall & HxGN Connect per applicazioni di Security e Public Safety"
Angelo CELANO – Hexagon's Geosystem Division – "Soluzioni hardware per migliorare la Situational Awareness"

UN CLOUD POSSIBILE PER LA DIFESA ITALIANA

2 dicembre 2021

Con il termine Cloud Computing si fa riferimento ad un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie internet, basati su risorse condivise, caratterizzati da flessibilità di utilizzo e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati a consumo. Un recente documento delle nostre istituzioni ha definito il trattamento dei dati della PA in Strategici, Critici e Ordinari e le tipologie di Cloud Computing in Public Cloud, Private Cloud, Hybrid Cloud e Multi Cloud.
Con riferimento alla Difesa appare evidente dover parlare di Dati Strategici e Private Cloud e quest'ultimo come l'unico possibile per la Difesa Italiana.
Ma cosa è il Private Cloud? Il Private Cloud consiste in Ambiente Cloud riservato per un'infrastruttura Cliente e per il suo uso esclusivo. Esso può essere di tipo "on -premises" o basato su una infrastruttura interamente inserita nel Dominio dell'Utilizzatore, il quale ne detiene il controllo e la completa responsabilità per la manutenzione e la sicurezza dei dati e dei servizi ospitati ed allocati presso le proprie strutture. Queste soluzioni mentre da un lato consentono una sicurezza pressoché massima dall'altra hanno lo svantaggio di non essere in grado di garantire un'adeguata scalabilità per gestire imprevisti picchi di domanda.
Il convegno ha cercato di tracciare una possibile linea di approccio per approfittare delle velocità, della bassa latenza e della capacità di storage dei dati che un cloud dedicato potrebbe dare alla Difesa Italiana nella totale security by Design.

Dott. Mariano VALLE - NCIA-NATO - NATO journey to cloud computing
Gen.B. Camillo SILEO - Stato Maggiore Difesa - La strategia di trasformazione digitale del Comparto Difesa
Ing. Giacomo SPERETTA - Leonardo - Approccio al go-to-cloud: una strategia per la gestione sicura della superiorità informativa
Ing. Pietro DELLA PERUTA - IBM Italia - Il prossimo salto del cloud: dall'ottimizzazione delle risorse a valore per la trasformazione
Ing. Stefano STINCHI – Microsoft - Come beneficiare dei vantaggi del Cloud senza compromessi sulla sovranità
Ing. Roberto DE FINIS – Almaviva - Cloud e Sovranità: Trade Off tra innovazione e controllo
C.F. Sebastiano NUZZI – COR-Difesa - Il Private Cloud della Difesa: Architettura e modelli di servizio in uso
Dott. Mirko LEANZA – Teleconsys - EDGE Private Cloud per applicazioni mission critical
Ing. Giuseppe LIETO – DigitalPlatforms - Automated deployable private cloud a supporto di missioni ed attività sul campo
Dott. Alessandro DI FELICE – OVHCloud - 12:40 Sovranità dei Dati nel Cloud
Dott. Leandro AGLIERI – VATES - Il ruolo di una soluzione di virtualizzazione Opensource, sicura e affidabile nel Cloud Computing

I contributi dei soci

THE IMPORTANCE OF OUR TRANSATLANTIC RELATIONSHIP REMAINS IMPERATIVE

June 2022

AFCEA INTERNATIONAL LTGEN(R) SUSAN S. LAWRENCE

Italy and Europe hold a special place in my heart because it was there that I commanded a brigade, overseeing two battalions in Germany, one in Belgium and another in Italy. This was my absolute favorite assignment during my entire time in the Army and prepared me well for the rest of my Army career and for now, at the helm of AFCEA International—the association for public and private sector professionals in cyber, defense, security, intelligence and related information technology disciplines.

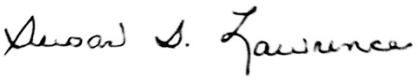
Together, our members and partners work for the safety and security of our nations.
The Rome Chapter, and all our chapters, are an important part of that important mission.

Over the past several months, the world has watched Ukraine face unprovoked attacks on its soil. In crimes against democracy, innocent lives have been lost, and many more are in danger. The strong Euro-Atlantic relationship is demonstrating itself the most important since the Cold War, and only while united with our allies can we resist all evil forces.

As believers in democracy and freedom, the United States and Italy share close ties and a strong relationship since before the establishment of Italy as a republic in 1946.
And though global challenges remain, it is important that our partnership and common values prevail. As key NATO allies, we have worked hand in hand to keep our nations secure from some of the world's largest threats.

Article 5 of the North Atlantic Alliance's treaty states that an armed attack on one is an attack on all. And in the case of such an attack on any single party, all NATO Parties will assist the attacked ally with "such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."
Today, however, security no longer solely refers to land, sea and air. Adversaries pose serious cyber threats, perpetually putting our national security at serious risk. Now the questions stand: will a cyber attack also trigger an Article 5 response? Should it? We must continue to emphasize the urgent need to strengthen our cyber defense, as industry leaders and members of our respective homeland security and intelligence communities. Vigilance and perseverance are paramount, but the key to a most secure world is partnership. As AFCEA members, we have the privilege of connecting with experts and allies around the globe and shape the conversations of global security. Together, we share knowledge through the exploration of issues relevant to both our nations, to work toward a safer tomorrow. With the help of our Italian friends and partners, may we work toward a more powerful and peaceful state.

Best wishes



Lt. Gen. Susan S. Lawrence, USA (Ret.)
President and CEO
AFCEA International

WHY DISRUPTIVE TECHNOLOGIES MATTER MORE THAN EVER IN DEFENCE

NATO's and EU's role, AFCEA's contribution

AFCEA EUROPE MAJGEN ERICH STAUDACHER

AFCEA turned 75 last year, almost a biblical age for associations. Already at the beginning of our unique association there was the strong interest of the military in learning about emerging technologies at that time. Ever since education and exchange on technology for defence and security were driving factors for AFCEA's mission to bring military/government, industry and academia together. Today, Armed Forces are in the midst of a huge digital transformation which leaves no branch and no service untouched. Software defined radios, battlefield management systems, digital workplaces, military app stores, satellite communications, but also 5G, hybrid cloud, edge computing. Cyber security and space have become inherent and indispensable aspects of all military systems and operations, they matured into domains of their own, by such underlining their importance. So much new technology, so much change and need for adaptation in the way the military acts and operates. And so much opportunities for AFCEA to assist…

Why now considering a whole new set of technology and call it "Emerging and Disruptive Technologies"?

I quote Mr. Mirco Geoana, DepSecGen NATO and Chairman of the NATO Innovation Board: "It's obvious that we are in the midst of the most intense technological race, not only in recent history but also, probably, in centuries. We must make sure that these new technologies work for us. And not against us. So it is essential that NATO Allies re-double our efforts to maintain our technological edge" and: "Working with the private sector and academia, Allies will ensure that we can harness the best of new technology for transatlantic security". And the EU tells us: "Remaining at the cutting edge of technological development is critical for ensuring Europe's prosperity, security, and way of life. New technologies are transforming the security and defence sectors at a faster pace than ever before and blurring the dividing line between the civilian and military domain."

The new technologies, in NATO's concept for the Defence Accelerator for the North Atlantic (DIANA) explicitly named as disruptive such as artificial intelligence, big-data processing, quantum-enabled technologies, autonomy, and space, and similar technologies, described in the European Defence Agency's Overarching Strategic Research Agenda (OSRA) or in other EU institutions' activities like the European Defence Fund and the Horizon Europe program are seen as decisive to innovations for prevailing in the peer-to-peer competition with Russia and China. At the same time, new operational needs arise for NATO, EU and their partners amongst western democracies, and result in the request for new capabilities such as Multi-Domain Operations Command and Control /JADC2 or operating under very degraded environmental conditions like in the Arctic. Also complexity and quantity of hybrid warfare incidents are increasing. Leading developments from civil industry or dual-use cases add to such innovative impulses for the military (e.g. smart textiles, IoT).

Last but not least, Cyber defence and its growing importance for the critical infrastructure, without this no military operation could be conducted, is a constant source of new technological applications

The current plans and activities of NATO and EU, monitored and supported by AFCEA Europe, offers a whole range of new opportunities for AFCEA on all levels of the association to continue its important work and serve its members by providing valuable information, renewed networking opportunities, attractive events. Discussing fascinating IT technologies and presenting the upcoming operational and business opportunities should also attract new members, in particular from the younger generations who may be more enthusiastic about this future of theirs and less concerned about "disruptions". Because the dramatic advancements in technology for sure will result in a shift of culture. Cultural and organizational questions also provide for a range of topics to be explored and discussed within the wonderful AFCEA network. The Rome chapter of AFCEA is well equipped for such an undertaking and certainly will serve their members and the whole community with exceptional events as traditionally. I wish the AFCEA Chapter Capitolo di Roma continued success in selecting the right and timely subjects for its impressive annual activities' programme, as it did in excellence during the past years. I am sure the members, sponsors, supporters will reward the chapter leadership by numerous presence at its various events.

https://www.afcea.org/site/?q=Staudacher

UTILIZZO DEL REMOTE SENSING NELL'INDIVIDUAZIONE DELLA LINEA DI RIVA

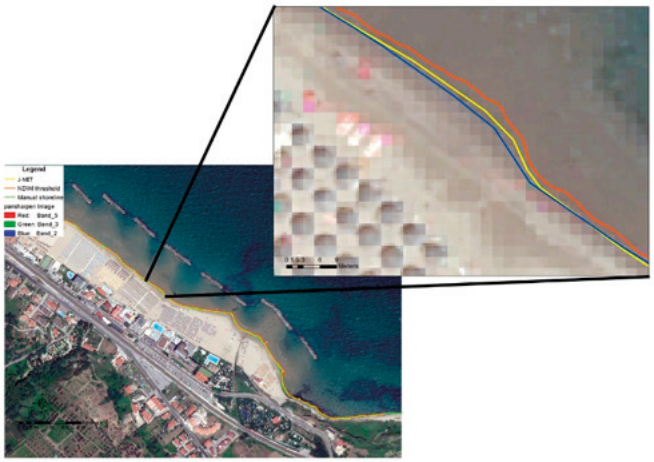
Donatella Dominici

UNIVERSITÀ DELL'AQUILA

La Prof. Donatella Dominici, vice presidente "università" di AFCEA Capitolo di Roma e membro del Women in AFCEA subcommittee, ha svolto un'interessante ricerca con un gruppo di ricercatrici (l'ing. Maria Alicandro e l'ing Sara Zollini) riguardante lo studio delle coste.

L'ambiente costiero sta subendo, nel corso del tempo, continui cambiamenti dovuti non solo alla sua natura dinamica ma anche a fattori geologici, geomorfologici, idrodinamici, biologici, climatici e antropici. Ad oggi, i fenomeni di erosione superano quelli di sedimentazione. Per questo il monitoraggio di tali aree è fondamentale per la salvaguardia del patrimonio culturale e delle popolazioni che vi abitano. La conoscenza delle dinamiche del litorale aiuta a comprendere un'ampia gamma di studi sull'area costiera, sulla sua gestione e pianificazione.
Condotto dal laboratorio di Geomatica del Dipartimento di Ingegneria Civile, Edile Architettura e Ambientale dell'Università degli Studi dell'Aquila, di cui la prof Dominici è responsabile scientifico, il progetto di ricerca si basa sull'integrazione di dati ottici e SAR per l'estrazione della linea di riva istantanea. In particolare, il progetto utilizza immagini satellitari ad alta (Sentinel-1 SAR e Sentinel-2 ottiche) ed altissima risoluzione (WorldView-2 ottiche), dati eterogenei provenienti anche dal Progetto Copernicus. La metodologia è stata testata su due siti costieri, Ortona (Chieti, Italia) e Castelldefels (Barcellona, Spagna).

La sperimentazione si è svolta seguendo una serie di fasi, prima di tutto la necessaria pre-elaborazione, essenziale per correggere distorsioni geometriche e radiometriche utili a ottenere un'immagine ortorettificata e georeferenziata. Successivamente sono stati testati diversi indici, algoritmi e filtri per analizzare in modo critico algoritmi già comunemente utilizzati in letteratura confrontandoli con nuovi algoritmi provenienti dal mondo dell'intelligenza artificiale. Tali algoritmi sono i Sistemi ACM (Active Connection Matrix), brevettati dal centro ricerche SEMEION e per la prima volta utilizzati in ambito territoriale. Per la validazione dei risultati sono state considerate, come verità a terra, la linea di riva estratta manualmente tramite ispezione visiva e un'altra tramite misure GNSS. I risultati hanno dimostrato che i Sistemi ACM, ed in particolare quelli chiamati Contractive Maps e il J-Net Dynamic, forniscono una migliore definizione ed estrazione della linea di riva, con precisioni dell'ordine del sub-pixel/pixel.
Un importante sviluppo di questa ricerca è stato quello di mettere a punto una nuova metodologia semi-automatica per l'estrazione della linea di riva istantanea, utilizzando prevalentemente immagini Sentinel come parte del programma Copernicus, che fornisce dati completi, liberi e gratuiti, facili da reperire ed utilizzare. Tali algoritmi hanno anche dimostrato un'ottima prestazione con il dato SAR, risultando meno sensibili all'effetto dello speckle.
La metodologia sperimentata può essere utilizzata per estrarre in maniera rapida le linee di riva di immagini catturate in istanti di tempo differenti e, quindi, valutarne l'eventuale cambiamento avvenuto.
Questo tipo di ricerca può proseguire su altri tipi di costa gestendo la fusione dei dati ottici e SAR sempre con il fine di facilitare la gestione di un piano di intervento da parte delle istituzioni a favore della salvaguardia del luogo.



"GUARDARE" CON LE ONDE RADIO

Potenzialità e prospettive

Ernestina Cianca

UNIVERSITÀ DI ROMA TOR VERGATA

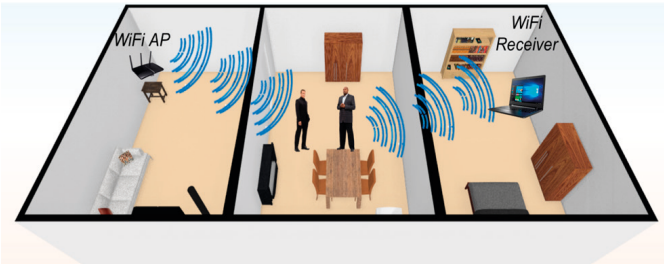
La Prof. Ernestina Cianca, consigliere direttivo di AFCEA Capitolo di Roma e membro del Women in AFCEA subcommittee, ha svolto un'interessante ricerca sul tema dell'RF sensing.

Siamo circondati da dispositivi che trasmettono segnali a radio-frequenza, WiFi, stazioni base della rete cellulare, smartwatch, stazioni televisive e Bluetooth della macchina, fornendo diversi servizi di comunicazione.

Recentemente, si è sviluppato un certo interesse verso il loro utilizzo come "collettori" di informazioni in un dato ambiente, si parla cioè di RF-sensing, e si intende la possibilità di usare segnali radio di opportunità per svolgere diverse attività di monitoraggio. Una di queste è il riconoscimento delle attività umane quali la presenza di una persona, se sta camminando, correndo, se sta seduta o è caduta, il riconoscimento dei gesti, il conteggio delle persone e il suo flusso all'interno di un ambiente.
L'RF sensing si basa sul principio che il canale di propagazione di un segnale a radio-frequenza è influenzato dalla presenza di una o più persone che riflettono le onde radio. Dall'analisi dei cambiamenti indotti al canale radio, è possibile quindi capire cosa succede in quell'ambiente. Tipicamente il riconoscimento viene fatto "allenando" un modello di Machine Learning (ML) che viene applicato alle "features" estratte in tempo reale dai segnali radio ricevuti., secondo due approcci principali:

- device-based, in cui la persona da monitorare indossa un rice-trasmettitore a radio frequenza, (un braccialetto, il proprio smartphone o smartwatch)
- device-free, in cui la persona non deve indossare nulla.

In entrambi i casi, si possono usare segnali presenti nell'ambiente oppure segnali specificatamente trasmessi per fare sensing. Il primo caso è più interessante in quanto utilizza infrastrutture già esistenti e richiede solo l'installazione di ricevitori che raccolgono le informazioni estraendole dal segnale ricevuto, trasmettendole eventualmente ad un server centrale per la fase di elaborazione
Il RF-sensing ha diverse applicazioni civili e militari. Infatti, può essere usato per il monitoraggio non invasivo di anziani in casa, capire le loro abitudini e correlarle a malattie con impatto sulla deambulazione; conteggio delle persone sia



per scopi di sicurezza sia per migliorare i flussi in un museo o supermercato attraverso la migliore comprensione di come si muovono le persone, rilevamento di persone attraverso i muri, pertanto potrebbe essere usato dalle forze dell'ordine o da militari per gestire situazioni in cui ci sono ostaggi, o da soccorritori che devono capire se c'è presenza umana sotto delle macerie.
Rispetto all'uso delle videocamere, questi sistemi sono meno invasivi e preservano la "privacy", inoltre l'angolo di vista è di 360 mentre la telecamera ha un angolo di vista limitato. L'attenzione verso questi sistemi è poi aumentata esponenzialmente con la pandemia da COVID-19 dove per molti servizi si è reso necessario contare in tempo reale il numero di persone presenti in ambienti interni.

Il Gruppo di Ricerca in cui lavora la Prof.ssa Ernestina Cianca è stato tra i precursori sul tema del RF-sensing. Nel 2020 è stato costituito uno spin-off universitario, dell'Univ. di Roma Tor Vergata[1] che ha come principale missione quella di sviluppare servizi ed applicazioni legate all'RF-sensing. Il gruppo ha lavorato sia su sistemi di activity recognition sia di conteggio delle persone, utilizzando diversi segnali radio, risultando tra i primi gruppi di ricerca ad utilizzare il segnale di opportunità LTE, trasmesso da una qualsiasi stazione base, per contare le persona in una stanza. Il ricevitore LTE utilizzato è una piattaforma SDR. È importante notare che per analizzare le variazioni del canale non c'è bisogno di una SIM card poiché vengono utilizzati dei segnali mandati in broadcast dalla stazione base. Il segnale WiFi è stato inoltre usato per "guardare" oltre i muri e in particolare, capire se ci sono persone ferme o in movimento. Nuove prospettive verranno aperte dai segnali radio previsti nei sistemi 5G e 6G. In particolare, i segnali a frequenze dell'ordine del Terahertz (TH), che si candidano a creare un unico sistema "radar distribuito" per fare sia comunicazione sia navigazione e sensing, giocheranno un ruolo chiave nella realizzazione di nuove applicazioni di Internet delle Cose, abilitando un monitoraggio "ubiquitous" e non invasivo, utile per applicazioni civili e militari.

[1] *www.radiopoints.org*

DIMENSIONE COGNITIVA E NARRAZIONE: COLLEGARE LE SINGOLE INFORMAZIONI NON BASTA

di R. De Finis

ALMAVIVA

Quarto Potere, il famoso film di Orson Wells che racconta la vita del cittadino Kane, faceva già capire nel 1941 quanto nelle democrazie moderne il potere delle informazioni, e della loro possibile manipolazione, fosse di fondamentale importanza e permettesse anche di accumulare, parallelamente, grandi ricchezze. A differenza dei canali di comunicazione raccontati nel film, quelli radio televisivi e della carta stampata, il canale offerto oggi dal Web, e dai Social Network più in generale, è ancora più potente perché permette non solo di comunicare con modalità più estese, in termini sia geografici che di quantità di contenuti, ma di costruire e mantenere con tutti gli utenti delle relazioni interattive puntuali estremamente più efficaci e ad un costo relativamente basso.

Oltre a permettere enormi estensioni e capillarità, il Web e i Social Network permettono infatti lo studio dei vari utenti con dati estremamente accurati e sempre aggiornati, rendendo possibile effettuare, con relativa facilità e velocemente, anche analisi descrittive e predittive delle preferenze dei singoli utenti (interessi, età, genere, geolocalizzazione, etc.) e delle loro aggregazioni (leader, follower, dimensione del gruppo, etc.)

Inoltre, grazie alle attività dei cosiddetti *influencer*, figure caratteristiche di questi nuovi tipi di canali di comunicazione, è molto più semplice costruire, sviluppare e mantenere, la necessaria fidelizzazione con decine di milioni di utenti. La creazione della fiducia nel Web diventa orientata al marchio piuttosto che al singolo prodotto; il meccanismo di costruzione della fiducia è strutturato e pianificato per realizzare una relazione costante e continuativa con gli utenti, per orientarne le preferenze, le decisioni e le azioni utilizzando il marchio come "scorciatoia" nella comunicazione.

L' introduzione negli ultimi anni della Intelligenza Artificiale nel settore della comunicazione digitale ha permesso di creare consenso, veicolando grandissime quantità di nuovi contenuti e informazioni molto dettagliate e anche personalizzate, automatizzando attività e flussi decisionali che prima dovevano essere svolti solo manualmente. L'applicazione della Intelligenza Artificiale (in particolare basata sugli algoritmi di *deep learning*) alla creazione dei contenuti ha determinato, in soli tre anni, una crescita esponenziale delle quantità prodotte (cfr. figura 2), raggiungendo un livello di qualità del contenuto molto simile a quello ottenuto con il processo umano. Questa potenza di calcolo permette di disporre velocemente, e a costi sempre più contenuti, di sistemi automatici intelligenti (*c.d. Bot*) per l'interazione con milioni di utenti permettendo una comprensione delle loro aspettative e del loro gradimento sempre maggiore e ottenendo una fidelizzazione sempre più costante.

Per portare solo alcuni recenti riscontri concreti degli effetti di rilevanza nazionale o internazionale causati dal utilizzo di campagne di informazione sul WEB e Social Networks, supportate da influencer e da algoritmi di intelligenza artificiale, si può citare l'articolo «*The role of bot squads in the political propaganda on Twitter*» dove è stata studiata l'attività di bot in relazione all'attività di campagna politica in Italia del 2018, oppure , ancora più recentemente, l'articolo "*Financial Markets and Social Media: Lessons From Information Security*" dove è stato analizzato un utilizzo dei Social Network e algoritmi di IA nel mercato finanziario mondiale. Nel secondo articolo viene descritta la speculazione attutata nel gennaio 2021 sulle azioni del rivenditore di videogiochi GameStop Corp. che ha generato, tramite una efficace azione di fidelizzazione da parte di un singolo influencer, una "bolla" con un massimo storico di $ 483, a partire da un iniziale prezzo di scambio di soli $ 20, per poi calare nuovamente a circa $ 40 in soli due mesi, causando una perdita agli investitori per miliardi di dollari e il fallimento della società GameStop Corp..

Queste nuove tecnologie trasferiscono la competizione tra organizzazioni (e Stati) dal dominio delle caratteristiche oggettive dei singoli prodotti o capacità offerte, al campo della dimensione cognitiva. La fiducia delle persone (nei prodotti che comprano, nei processi elettorali, nelle istituzioni nazionali, negli alleati, nella classe politica) diventa l'obiettivo delle strategie di *digital influence* perpetrate dai *competitors* che, avvalendosi dei modelli di interazione tra gruppi sociali sul Web, già esistenti o creati ad hoc, promuovono la diffusione di contenuti finalizzati a generare un determinato effetto nella dimensione cognitiva e "manipolare" tramite esso le reazioni e il comportamento di una specifico gruppo di persone. I

meccanismi di creazione della fiducia e del consenso su un particolare messaggio o, più in generale idea, sono complessi e si basano sullo sfruttamento dei cosiddetti *bias* cognitivi durante la campagna di comunicazione. I *bias* cognitivi sono veri e propri errori che il nostro cervello commette abitualmente e si basano su una percezione parziale della realtà, su pregiudizi che, ogni giorno, influenzano i nostri pensieri e il nostro potere decisionale: sono meccanismi inconsci originati dall'evoluzione delle capacità cognitive dell'uomo durante la sua crescita e costituiscono la scorciatoia preferita del cervello umano per processare velocemente le informazioni ricevute.

Il confronto portato nell'ambito della narrativa, pertanto, non si inquadra sulla descrizione di un evento o fatto in quanto tale, ma sul significato e l'effetto emotivo dei fatti presenti nell'informazione e alla loro interpretazione nel tempo. L'idea alla base della strategia di comunicazione è di creare una storia che porti alla conclusione desiderata nella visione delle persone a prescindere dalla sua veridicità. Questa deve incontrare il favore dell'audience di riferimento, già preparata da una specifica base di influencer o marchi di fiducia, al punto che la sua efficacia dipende dalla capacità di eludere il pensiero critico, sviluppato con lo studio analitico delle fonti, plasmandone l'identità e, di conseguenza, le sue convinzioni e azioni. Un esempio recente di competizione nel dominio cognitivo è la narrazione del conflitto Russo-Ucraino, costruita, anche prima del conflitto stesso, via Web e Social Network, e, conseguentemente, anche sui media più tradizionali, come narrazione emotiva piuttosto che come semplice descrizione dei fatti. In questo conflitto è stata data importanza alle percezioni sociali degli eventi oltre che all'effettivo utilizzo di mezzi bellici. I due schieramenti hanno inquadrato la narrazione per influenzare il processo decisionale, la comunicazione politica e l'evoluzione del dibattito pubblico a proprio favore su un argomento altamente polarizzante e divisivo come una guerra.

Il contrasto alla manipolazione o alla disinformazione non può essere condotto solo attraverso attività di "smentita" e evidenziazione dei fatti oggettivi. Tale soluzione, limitandosi alla parte razionale dell'informazione, si rileva inefficace e con possibilità di sfociare addirittura in azioni controproducenti percepite, dal punto di vista emotivo, come tentativi di "insabbiamento" o limitazione della libertà di pensiero e espressione. Un'azione alternativa è quella di identificare la linea di narrazione del *competitor*, dalle sue premesse alle possibili conclusioni, riconoscerne il processo interpretativo e i *bias* cognitivi sfruttati, in modo da identificare una traiettoria. In questo modo si può anticipare la linea narrativa del *competitor* e intervenire inserendo altri

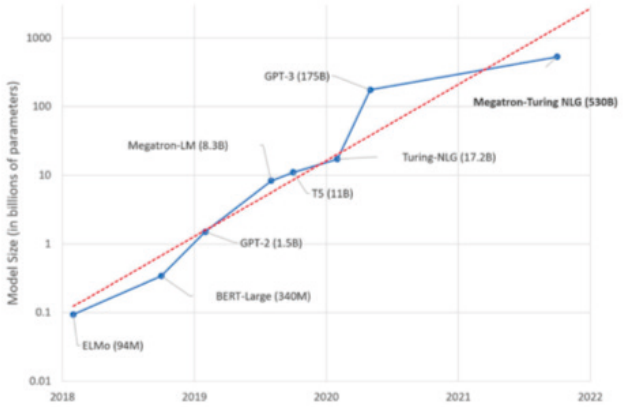


Fig. 2 - Crescita IA (Fonte: Microsoft Research 2021)

elementi e fatti che riportino l'effetto verso una descrizione più autentica rafforzando la fiducia nella propria linea di consenso, che deve essere già stata delineata, rendendo la fonte della narrazione del *competitor* non efficace.

La capacità della *digital influence* delle masse tramite l'interpretazione delle informazioni, con nuovi e potenti asset tecnologici, evidenzia quindi la centralità del dominio della dimensione cognitiva, rispetto alle altre dimensioni nei moderni conflitti. La comunicazione strategica, agendo direttamente sulla sfera emotiva piuttosto che su quella razionale, è risultata essere, nella attuale prospettiva di confronto a bassa intensità di conflitto, una arma formidabile, a basso costo, e accessibile da molte organizzazioni.

E' comunque da evidenziare che la mole di informazioni disponibili e in continua crescita sul Web e sui Social Network renderanno sempre più difficile per il singolo utente farsi una propria opinione informata e analitica rendendolo comunque soggetto a una crescente fluidità di azione e instabilità decisionale. Una vera contromisura a questa tendenza purtroppo è difficile da realizzare perché può essere solo di lungo periodo e basata sul mantenimento di un pensiero critico, sulla continua ricerca delle fonti e dal confronto aperto e costruttivo tra pensieri diversi. Diventa quindi fondamentale ancora di più per uno Stato libero investire in una istruzione multidisciplinare e multiculturale per tutto il periodo di formazione, dalle scuole dell'infanzia fino all'università, e mantenere nel tempo, anche attraverso uno più periodi obbligatori di servizio pubblico civile o militare, momenti di aggregazione e partecipazione alla vita sociale del Paese reale e non solamente virtuale.

Solo una solida coscienza valoriale comune basata sui principi democratici di libertà, prosperità e uguaglianza rappresenterà il vero baluardo a questi tipi di "attacchi" che cercheranno di minare sempre di più le basi del vivere civile assoggettandolo alla opportunità del momento.

IL SUPPORTO TECNICO-AMMINISTRATIVO NELL'ACQUISIZIONE DI PRODOTTI E SISTEMI INNOVATIVI

BMA, valori ed esperienza trentennale al servizio del Paese nel settore dell'alta tecnologia

B.M.A.

L'acquisizione di prodotti e sistemi da ditte estere specializzate nell'alta tecnologia e nell'innovazione è sicuramente attività difficile e complessa per le Agenzie Governative di Procurement. Ciò perché si tratta di generare Capitolati Tecnici a partire dai requisiti tecnico-operativi originati dagli Enti operativi e formule contrattuali in linea con la giurisdizione internazionale che siano atte a garantire la tutela dello Stato dal punto di vista della rispondenza prestazionale dei prodotti e sistemi acquisiti e dal punto di vista legale contrattuale per la garanzia di tutta la vita del prodotto o del sistema. La BMA offre un'esperienza trentennale al servizio della difesa, della protezione civile, della sicurezza e dell'industria nazionale primaria rappresentando in Italia aziende estere che operano in settori a tecnologia avanzata. Nel corso degli anni BMA ha realizzato importanti collaborazioni internazionali e fornisce continuo supporto agli Enti governativi di Procurement, di Supporto Logistico ed ai Reparti Operativi. La direzione aziendale insieme ad un team di ingegneri e di personale specializzato svolge tutte le procedure atte alla fornitura al Ministero della Difesa, al Ministero degli Interni e a Ditte leader nazionali di prodotti e servizi unitamente alla traduzione di manuali tecnici, alle procedure di codifica e classificazione dei materiali, all'assistenza durante i corsi di formazione e addestramento del personale sui sistemi introdotti in servizio, con traduzione simultanea e di materiale didattico. Organizza e facilita gli incontri ed i colloqui tra le ditte rappresentate ed il personale governativo o industriale.
I principali settori operativi della BMA sono:

VISIONE NOTTURNA

Visori ad alta tecnologia per l'aviazione e le forze terrestri, telecamere, termo camere, torrette multi-sensori girostabilizzate.

F 4949

F 5032

F 6025

BMA rappresenta in Italia società specializzate nel settore della visione notturna ed in particolare la società americana Elbit Systems of America che esprime con i suoi prodotti la sintesi evolutiva delle tecniche e delle tecnologie del settore.
I prodotti più significativi sono l'F5032 – AN/PVS 31D che è un visore binoculare per impiego terrestre con tecnologia ad intensificazione di luce caratterizzato da peso ridotto, messa a fuoco ed autonomia unici nel settore.
L'F6025 – ENVGB visore binoculare per impiego terrestre modulare integra la tecnologia ad intensificazione di luce con la visione a infrarossi.
Infine l'F4949 – AN/AVS-9 un visore binoculare per impego aeronautico con tecnologia ad intensificazione di luce.

CBRN

Strumenti per il rilevamento e l'identificazione chimica, batteriologica, radiologica e nucleare.

JSAM

AP4C+

TOM 87

SPIR ACE

BMA rappresenta in Italia le principali aziende europee leader nel settore CBRN capaci di coprire con i loro prodotti le esigenze nel settore.
Esempi di prodotti innovativi per la protezione fisica dell'operatore sono la maschera JSAM (Joint Service Aircrew Mask) per la protezione completa CBRN dell'equipaggio

in campo aeronautico e la tuta permeabile TOM 87 per la protezione CBRN dell'operatore in campo terrestre.
Tra gli strumenti l'AP4C+ leggero e compatto consente per la rilevazione della minaccia chimica e lo SPIR ACE che rileva ed identifica la minaccia radiologica e nucleare.

DEMILITARIZZAZIONE E PROTEZIONE
Sistemi per la bonifica, la protezione e la demilitarizzazione di munizioni convenzionali e chimiche.

SDC1200+OGT

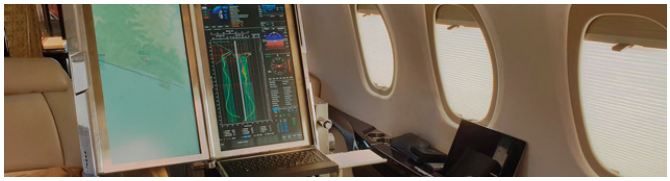
DynaSEALR X

BMA rappresenta la società Dynasafe specializzata nella progettazione, realizzazione e messa in servizio di complessi impianti completi di tutte le opere necessarie per fornire e manutenere la capacità di demilitarizzazione del munizionamento speciale con la massima sicurezza operativa ed ambientale.
L'impianto SDC1200+OGT selezionato per l'Italia permette la demilitarizzazione di munizionamento convenzionale e chimico è già operante in diverse nazioni Europee ed extraeuropee da molti anni.
Le camere a contenimento DynaSEALR X sono progettate per le squadre EOD allo scopo di conservare, trasportare o risolvere in sicurezza ordigni chimici e convenzionali.

AEROMOBILI A PILOTAGGIO REMOTO (APR)
Aeromobili a pilotaggio remoto per attività di Intelligence dotati di sensori avanzati per ricognizione, sorveglianza e acquisizione obiettivi.

Il Sistema Micro-APR RAVEN.
È uno strumento di sorveglianza e ricognizione a lancio manuale, che concorre ad accrescere la Situational Awareness attraverso l'acquisizione di immagini e video, in real time, dell'Area di Responsabilità.
BMA rappresenta la società americana AeroVironment che sviluppa e produce questi sistemi e supporta gli Enti governativi Italiani preposti all'Acquisizione, alla Certificazione per Aeronavigabilità e Qualifica ed agli Enti operativi che li impiegano.

SISTEMI RADIOMISURE
Sistemi per il controllo delle radioassistenze al volo.



Il Sistema UNIFIS 3000 per le RadioMisure

Radar, VOR, DME, ADF e ILS sono alcune delle sigle degli apparati di radionavigazione aerea che utilizzano segnali elettromagnetici capaci di fornire al pilota le informazioni essenziali circa la posizione e l'assetto del velivolo sui piani orizzontale e verticale. I sistemi RadioMisure permettono di verificare l'accuratezza dei segnali emessi dalle stazioni a terra in modo da garantire agli operatori del trasporto aereo di volare in assoluta sicurezza.
BMA rappresenta la società norvegese Norwegian Special Mission che ha sviluppato e fornisce i sistemi RadioMisure migliori al mondo per tecniche e tecnologie impiegate e che l'Aeronautica Militare Italiana e l'ENAV, gli Ente Italiani preposti al controllo dei sistemi di assistenza al Volo hanno selezionato. I sistemi RadioMisure sono installati a bordo dei velivoli Piaggio P-180 appositamente modificati ed equipaggiati per l'esecuzione dei controlli in volo nel rispetto delle normative internazionali.

SIMULAZIONE E TEST PER LA DIFESA E LO SPAZIO: SOLUZIONI SW, HW E METODOLOGIA DA UTILIZZARE

Soluzioni CRISEL con i partner CS, Hensoldt, Spirent

CRISEL

Crisel opera in Italia nel settore della innovazione tecnologica in ambito Geospatial, Aerospazio e Difesa.
L'ambito di innovazione a seconda del settore coinvolge SW, HW e metodologia di misura. Di seguito riportiamo i risultati delle soluzioni ottenuti con le nostre partner CS-Group, Hensoldt Nexeya e Spirent rispettivamente nella Simulazione di Trasmissioni Tattiche, Flight Test e Simulazione per il Test di Ricevitori GPS/GNSS.

Link16 Live Virtual Constructive (LVC) system CS GROUP.
Questo sistema di addestramento tattico, creato da CS GROUP (www.csgroup.eu) su richiesta della French Joint Forces, è dotato di una simulazione costruttiva L16, a cui possono aderire partecipanti dal vivo e virtuali, può essere utilizzato per l'allenamento quotidiano e le esercitazioni multi-sito in più ambienti.
Integra l'ambiente live con quello virtuale in scenari realistici con Link 16, in base alle esigenze della sessione di addestramento, fornendo un addestramento operativo più efficiente ed economico per le forze aeree, poiché evita di utilizzare velivoli reali ed è in grado di proporre dall'addestramento di base a quello avanzato. Grazie al realismo dei suoi scenari di addestramento, il sistema LVC consente di arricchire la situazione tattica, in particolare con la capacità di simulazione delle entità partecipanti L16, partecipare in diverse aree di combattimento con forze rosse, blu e bianche ed eseguire debriefing.
Il sistema si basa su un'architettura aperta e può implementare diversi prodotti di CS GROUP come DirectCGF (Computer Generated Forces di CS GROUP) per definire gli scenari e gestire l'addestramento costruttivo, FIGHTERX (Virtual Fighter), STARLINX (command & control TacticalDataLink system), integrato da un sistema multisito After Action Review. I partecipanti dal vivo (aerei, navi...) sono collegati tramite terminali MIDS di terra. Il sistema LVC è aperto alla connessione (protocolli standard come DIS/HLA/SIMPLE) con addestratori virtuali che eseguono velivoli simulati, navi o piattaforme di terra. I sistemi legacy possono anche essere collegati tramite gateway.
Questo sistema LVC è regolarmente utilizzato dalle forze francesi per addestrare piloti e controllori in scenari aria-aria e terra aerea per esercitazioni nazionali e multinazionali (compresa la NATO). CS GROUP è un'azienda francese innovativa di medie dimensioni, con 202 milioni di euro di fatturato e 2000 dipendenti, con un alto livello di competenza tecnica e professionale, fornisce sistemi intelligenti nel campo della difesa e della sicurezza.

Una transizione verso il futuro dei flight test: software di elaborazione dati HENSOLDT NEXEYA (www.hensoldt.net) MAGALI Chapter 7
La metodologia Chapter 7 è stata introdotta negli standard di telemetria dei flight test (IRIG106) nel 2015 con lo scopo di semplificare l'architettura di bordo per le fonti di dati asincrone pur utilizzando l'hardware legacy del Chapter 4 a terra. Inoltre, questo nuovo protocollo beneficia del crescente utilizzo del popolare software di elaborazione Chapter 10. Le varie fonti di dati di bordo vengono acquisite e incorporate in un flusso di dati PCM standard Chapter 4. Qualunque sia il tipo di dati e lo scopo (sviluppo di aeromobili, test di volo, monitoraggio dello stato di salute sui voli operativi ...), la tendenza è ora quella di produrre e archiviare un grande volume di dati diversi. Di fronte a questo ampio pannello di formati da elaborare, le persone che sviluppano aeromobili o test di volo hanno bisogno di strumenti efficienti per impostare le loro prove e concentrarsi su dati utili. Oltre al materiale utilizzato dai test range (a bordo o a terra), il software di elaborazione dati per test di volo (DPS) è una parte fondamentale di questo processo.
Il Chapter 7 consente il trasporto di dati Ethernet grezzi utilizzando parti specifiche di un frame del Chapter 4. Questi frame "grezzi" sono tipicamente utilizzati per trasportare Video Over IP o dati attraverso protocolli Network come IENA, iNET ecc ... La maggior parte dei dati temporali sono copie singole dei dati Ethernet del sistema di bordo (bus di sistema, comunicazione tra apparecchiature ...).
Le principali sfide affrontate nell'integrazione del Chapter 7 dell'elaborazione dei dati in MAGALI sono:

- Gestione di un ampio set di dati e protocolli diversi con un buon livello di prestazioni;
- Tolleranza al bit error durante la trasmissione;
- Il Multi-source time synchronization;
- Raw data storage and data gateway. Tutti i pacchetti raw memorizzati vengono anche trasmessi in UDP in modo che il sistema possa essere utilizzato come gateway da Chapter 7 a IP in tempo reale;
- Fornire un setup user-friendly con una configurazione facile e automatica e la possibilità di importare direttamente le configurazioni di prova da terra;

MAGALI Chapter 7 Data Processing System può essere utilizzato come il cuore dei sistemi di terra di telemetria di

nuova generazione. In conclusione, Chapter 7 semplifica le architetture di bordo e di terra. Riduce anche il tempo dedicato all'impostazione della missione. Si adatta quindi perfettamente al trasporto di dati asincroni (video, bus digitali...) mescolati con un insieme di dati sincroni (dati analogici). Chapter 7 è un formato a prova di futuro ed è la transizione perfetta dalle architetture legacy al futuro della telemetria in cui lo standard full IP quasi sicuramente sarà il più diffuso. HENSOLDT NEXEYA sviluppa soluzioni di flight test con l'obiettivo principale di seguire le nuove tecnologie mantenendo la compatibilità con le installazioni legacy.

Missioni commerciali con i satelliti CubeSat: perchè testare il ricevitore GPS/GNSS di bordo con un simulatore è così essenziale?

I satelliti CubeSat contengono ricevitori GPS/GNSS per la determinazione dell'orbita e della sincronizzazione temporale e lo sviluppo di questa tecnologia ha fatto sì che le prestazioni del ricevitore GNSS integrato a bordo vadano testate in laboratorio utilizzando dei validi scenari operativi.

È fondamentale eseguire test di posizione, navigazione e sincronizzazione

Una funzione peculiare è la determinazione ed il controllo sia dell'altitudine che dell'orbita, al cui scopo si utilizza un ricevitore GPS L1. I satelliti che volano in formazione possono anche utilizzare i dati del ricevitore GPS/GNSS per coordinare la propria posizione reciproca nella stessa costellazione e per sincronizzare le operazioni fra di loro.

La simulazione è l'unico modo per testare rigorosamente le prestazioni PNT - Posizione Navigazione Tempo - prima del lancio

I test con i segnali GNSS in tempo reale sono inaffidabili per valutare le prestazioni. Le condizioni in orbita terrestre bassa (LEO) sono molto diverse da quelle sulla Terra ed il ricevitore dovrebbe muoversi a diversi km/s. La simulazione in laboratorio di segnali GNSS è il metodo di prova preferito per le applicazioni commerciali, militari e spaziali più consolidate.

Funzionalità da testare con la simulazione GNSS

Uno dei parametri da testare con il simulatore è il segnale Doppler: un CubeSat che opera in LEO vola ad una velocità di 7 km/s. Il ricevitore GNSS deve essere in grado di gestire lo spostamento Doppler fra il movimento del CubeSat e il movimento dei satelliti GPS. Questo è un esempio di una capacità impossibile da testare prima del lancio poiché la velocità richiesta non può essere raggiunta a terra.

Determinazione precisa dell'orbita (POD)

L'accuratezza dell'orbita utilizzando un ricevitore GNSS può variare da pochi metri a pochi centimetri, a seconda della classe di ricevitore impiegato. Il POD si ottiene anche effettuando frequenti misurazioni GPS o GNSS in laboratorio. La simulazione consentirà agli ingegneri di determinare il tipo di dati e la frequenza di campionamento ottimali da utilizzare affinché il loro algoritmo di posizionamento raggiunga la precisione richiesta.

Prestazioni dell'antenna

Le prestazioni dell'antenna (o delle antenne) sono legate al diagramma di radiazioni, alla posizione di installazione e al multi-path, i cui test di simulazione in camera anecoica forniranno informazioni utili in fase di sviluppo.

Sincronizzazione

I CubeSat sono costituiti da più sottosistemi che necessitano di funzionamento sincrono. Il segnale orario ricevuto dal ricevitore GNSS LEO, viene utilizzato per l'ora e la sincronizzazione. La simulazione consentirà ad esempio di sincronizzare con precisione le manovre in volo di formazione.

Eventi speciali

I CubeSat progettati per missioni di lungo periodo potrebbero incontrare eventi non previsti. Uno di questi è l'inserimento occasionale di un "secondo intercalare" nel segnale orario GPS, per riportare l'ora coordinata universale (UTC) in allineamento con la rotazione terrestre. Gli sviluppatori verificano che il ricevitore possa gestire correttamente gli inserimenti del "secondo intercalare", azione apparentemente banale da simulare ma impossibile da testare in ambiente reale.

Gestione delle interferenze a bordo

La dimensione contenuta dei satelliti riduce la distanza tra il ricevitore GNSS e i componenti dei circuiti del satellite. Il rumore RF generato da questi componenti potrebbe interferire con le frequenze GNSS, motivo per il quale testare la robustezza RF del ricevitore/antenna è fondamentale.

Spirent (www.spirent.com) ha oltre 25 anni di esperienza e competenza nelle applicazioni spaziali e della difesa.

Le soluzioni di test PNT di Spirent non contemplano l'opzione fallimento ed invece offrono il controllo, la precisione e la affidabilità necessarie ad evitare guasti imprevisti e costosi, superando le sfide uniche dello spazio. Dallo sviluppo di nuovi segnali GNSS alla determinazione dell'orbita di precisione, i sistemi di simulazione Spirent sono stati progettati per lo sviluppo della prossima generazione di tecnologia spaziale.

DP PER LA DIFESA ITALIANA E LA NATO

DIGITALPLATFORMS

DigitalPlatforms SpA (DP) è un gruppo industriale italiano, in rapida crescita, che opera nel settore dell'Internet of Things, della CyberSecurity e delle tecnologie per la trasformazione digitale e della Difesa. Il Gruppo DP è composto da sette aziende/BU tutte basate in Italia, con una storia industriale compresa tra i 20 ed i 50 anni nel proprio settore di competenza e impiega circa 400 dipendenti. Amiamo produrre!!!!

DP è un player full liner, presente in tutti gli elementi necessari per realizzare soluzioni IoT end-to-end. DP parte dallo sviluppo, ideazione e produzione di sensori e prodotti di elettronica industriale, passando per i sistemi e le tecnologie di comando e controllo, fino alle piattaforme IoT, al system integration IT,alla Cybersecurity e all Intelligenza Artificiale. Ciascuna delle aziende operative che fanno parte del Gruppo DP presidia uno dei diversi elementi della catena del valore della soluzione IoT/Cyber/Defense.

Le soluzioni e i prodotti Tempest

Nel mondo difesa ci caratterizziamo come il più importante fornitore di Soluzioni Tempest Italiano per la Difesa con un investimento di ben due camere schermate per la tempestizzazione militare A, B, C di differenti apparati ICT. Questo investimento che può operare su più turni ci mette nella lista dei maggiori operatori Tempest della Nato.

Infrastrutture Certificate e Valutazione Ce.Va per la Security by Design dei sistemi per la Difesa

Infrastrutture classificate e non classificate: progettazione e realizzazione di infrastrutture di rete sicure, soluzioni per il trattamento dei dati in ambienti classificati (incluso il multilivello) e non classificati, soluzioni di Disaster Recovery e attraverso i nostri laboratori di valutazione Ce.Va portiamo a classifica militare processi, procedure, prodotti di terze parti, attuando un percorso virtuoso di Security by Design al servizio della progettazione di sistemi militari.

DP opera inoltre nel campo del Hardening, irrobustendo sia a livello hardware che software device ed ICT equipment del cliente finale.

Le soluzioni di Cyber Security per la Difesa

Risk & Vulnerability Assessment, analisi delle vulnerabilità, valutazione della sicurezza, crittografia.

Audit e valutazione, Governance e conformità, Sicurezza e privacy, Supply chain Safeguard. Intelligence sulle minacce cyber, Penetration Test, V. A, Red Teaming, Sistemi di Cyber Awarness per il personale, Cyber Training & Coaching, Architetture di sicurezza, Continuità e ripristino di emergenza servizi digitali. SIEM e gestione dei registri, Gestione delle identità e controllo degli accessi, Gestione dei contenuti, Prevenzione della perdita dei dati, Sicurezza convergente IT/OT, Custom IOT, Sistemi di Osint/Closint. Analisi della vulnerabilità del Software Open Source . Analisi malware e cyber threat, Soluzioni di cyber-attack attribution e Leakage and in siding monitoring.

Le soluzioni di Intelligenza Artificiale per la Difesa

DP ha recentemente dato vita ad una nuova line di prodotti che utilizzano AI ed il Machine Learning come base tecnologica. Tra le varie applicazioni effettive abbiamo già messo a punto: sistemi di manutenzione predittiva, sistemi di controllo territorio e aree urbanizzate o controllo sedime, sistemi di controllo per mezzi in avvicinamento, sistemi di autenticazione multi fattore per la comunicazione sicura, sistemi di video intelligence ed analisi contenuti internet o broadcast. Identificazione e lettura di firmware alieni/ avversari a prescindere dalla sorgente.

ELES S.P.A. CRESCITA CONTINUA NEL SETTORE DELL'AEROSPAZIO E DIFESA

ELES SEMICONDUCTOR

Eles S.p.a., azienda leader nell'ambito del controllo dell'affidabilità e della qualità dei semiconduttori, con importante presenza nel settore Difesa Italiano ed Europeo con la divisione Aerospace&Defence, ribadisce la presenza e la propria strategia di crescita per linee esterne grazie al M&A con focus su aziende complementari con importante portafoglio clienti a livello nazionale ed Europeo.

In quest'ottica, nel corso dell'ultimo anno ELES S.p.a. ha perfezionato due nuove acquisizioni, con l'obiettivo di concretizzare una spinta sempre più forte verso una significativa diversificazione settoriale grazie alla replicazione dell'offerta di soluzioni per l'affidabilità dei semiconduttori da applicare anche ai moduli elettronici ed alle centraline di controllo (ECU, INFOTAINMENT,...).

Le due acquisizioni nello specifico hanno riguardato:

- la società CAMPERA-ES, azienda con sede in Livorno ed operante nel settore Aerospace & Defence dal 2014, fornitore qualificato di sviluppi ed Intellectual Property (IP) per Video, Radar, Mission e Safety Critical Systems su FPGA e su tecnologia System on Chip. Impresa con altissimo potenziale di crescita proprio in virtù dell'IP sviluppato ed esportabile tout court agli altri clienti in portafoglio alle aziende del gruppo.
- la società CBL Electronics, azienda sita in Todi, operante nel settore Aerospace & Defence dal 2002, protagonista nel settore della progettazione Elettronica e capace di gestire l'intera filiera produttiva, dalla progettazione alla realizzazione e messa in esercizio del prodotto finale: progettazione hardware e software, firmware, meccanica, simulazione, progettazione CAD layout, sviluppo di sistemi complessi e programmi di test, supporto ai test di funzionalità ed affidabilità. Anche in questo caso la società ha in pectore un forte sviluppo potendo offrire ai propri clienti soluzioni di final test su moduli e centraline basate sull'IP R.E.T.E. (Reliability Embedded Test Engineering) di Eles S.p.a.

Grazie a queste due importanti acquisizioni, ELES S.p.a. mira ad un rapido consolidamento come realtà industriale con un ottimo portafoglio clienti ed ordini e quindi grande gruppo industriale HI-TECH, capace di fornire al mercato un'offerta ampia e diversificata. Oltre a questo, le sinergie attese dall'integrazione delle due aziende acquisite riguardano sia una significativa razionalizzazione organizzativa che l'espansione di fatturato, ed anche una importante cost reduction come gruppo di acquisto rendendo ulteriormente interessante la remunerazione dalle vendite.

Eles S.p.a. ha da sempre posto al centro della sua proposta il cliente e la soddisfazione dei suoi bisogni espliciti ed impliciti; proprio con il supporto di consulenza R.E.T.E. applicato alle soluzioni Campera e CBL intende replicare verso una platea molto più ampia i successi ed benefici di un approccio strutturato al design ed all'affidabilità a 360°.

Solo con l'adozione della filosofia R.E.T.E. di Eles S.p.a. si potrà tendere al raggiungimento dello "Zero Defect" verso il cliente finale sia che si parli di semiconduttori, sia che si tratti di moduli elettronici e centraline di controllo (ECU).

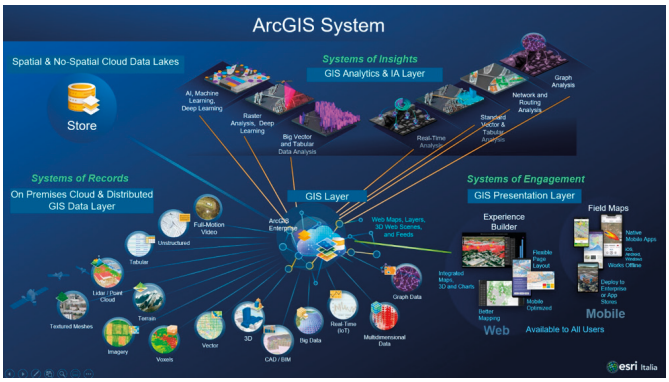
NUOVE TECNOLOGIE GIS PER LA SITUATIONAL AWARENESS, LA LOCATION INTELLIGENCE E GLI ANALYTICS

Esri ArcGIS System al servizio della Difesa

ESRI ITALIA

Esri, società leader a livello mondiale nella Location Intelligence e promotrice della "The Science of Where", propone un unico sistema geospaziale che supporta a 360 gradi la realizzazione di servizi per la Difesa. Un Sistema aperto e collaborativo, in rapida e costante evoluzione, volto ad integrare e valorizzare un ampio set di tecnologie innovative. Il punto di partenza è il **GIS Data Layer**: un "*Sistema di Records*" che vede protagonisti i Big Data con le sue matrici multidimensionali, dove grandi quantità e tipologie di informazioni spazio-temporali estendono e applicano il concetto di "location" tradizionale a nuove entità, ad esempio, filmati di rilevamenti, immagini da drone e documenti non strutturati (spesso elaborati in tempo reale tramite web harversting). Anche la rappresentazione tradizionale del territorio 2D/3D/4D si amplia grazie al Digital Twin, dove il dato non serve solo a ritrarre in forma estremamente realistica ogni dettaglio degli assets, ma ad evidenziare il "comportamento", "le regole e le relazioni" tra gli oggetti. Il dato è così governato da un'informazione intelligente. L'analisi e la rappresentazione dei teatri operativi si evolve con la Situational Awareness, arricchita dai sistemi predittivi. L'intelligenza Artificiale applicata al territorio prende sempre più spazio negli algoritmi di analisi spaziale tradizionale, diminuendo il gap tra GIS Data Layer e GIS Analytics Layer, con un modello di deep learning che rappresenta il dato stesso.

Il **GIS Analytics Layer** è il vero motore del Sistema Esri ArcGIS, configurato come un "System of Insights". I server GIS sono sempre più efficienti nel cogliere e analizzare ogni caratteristica del dato e le sue relative evoluzioni, che avvengono con grande velocità. Il Raster Analytics Server, ad esempio, non solo mosaica e rappresenta direttamente su web enormi quantità di immagini provenienti da innumerevoli fonti, ma analizza in real-time la profondità spazio-temporale dell'informazione, raccontandoci, cosa, dove, quando e quanto muta sul territorio. Oltre alla detection di ogni oggetto che si muove sul territorio, si analizzano le relazioni tra oggetti, entità e contesti. In questo modo, oltre alla creazione di mappe



tematiche dinamiche, i server di analisi GIS generano e gestiscono scenari predittivi di tipo "what if", che vanno ben oltre la creazione di mappe tematiche dinamiche.

Il **GIS Presentation Layer** del Sistema Esri ArcGIS è un insieme di tecnologie di "Engagement" di ultima generazione. Analisi avanzate di dati complessi, soggetti a numerose e rapide variazioni, richiedono, infatti, visori in grado di sfruttare al massimo hardware e schede grafiche potenti ed ottimizzate. Grazie ad API e software Developer Kit (SDK), già certificati NATO e messi a disposizione da Esri, tali fattori vengono affrontati e risolti a basso livello, senza la necessità di processi di programmazione complessa. Alle API e SDK si sovrappongono framework di presentation, con tecnologie e linguaggi di programmazione standard di mercato, completi di widgets funzionali e strumenti di rappresentazione che semplificano enormemente lo sviluppo, fino ad avere applicazioni pronte all'uso. Questo modello, non solo abbatte i tempi e i costi di implementazione, ma permette agli enti della Difesa di formare velocemente il proprio personale per gestire e sviluppare in autonomia le applicazioni e i portali, adeguandole sempre al passo con i tempi. La rappresentazione in mappa del territorio e delle situazioni (spesso arricchita con dashboard, documenti e filmati) estende il concetto di digital twin anche al "Presentation Layer", spesso con l'ausilio di device per la realtà aumentata (AR), realtà immersive (IR) e realtà virtuale (VR). Le mappe e i cruscotti, con tutte le simbologie militari supportate (terrestri, navali, aeree), si basano sul concetto di "Smart Mapping", incentrato sulla comprensione immediata di fenomeni ed evoluzioni che cambiano in fretta, elemento prioritario per il supporto alle decisioni.

Le **applicazioni Esri desktop professionali** (ArcGIS PRO) dispongono da sempre di **"Military Tools"** e di estensioni verticali specifiche per l'analisi e la rappresentazione nel mondo defense (Aviation Charting, Defense Mapping, Maritime, Production Mapping, ecc.)

La veloce condivisione sul campo delle informazioni tra i reparti è supportata dal Sistema ArcGIS con l'offerta di software per ogni ambiente operativo: Desktop e Web per gli uffici e *mobile* per le applicazioni sul campo. I sistemi godono dello stesso modello di riferimento sopra citato, vale a dire, librerie, interfacce e funzionalità pronte all'uso ed efficienti per la condivisione in sicurezza (certificata) delle informazioni tra i vari sistemi.

Esri mette a disposizione l'utilizzo di un unico sistema con modalità operative altrettanto uniche: una delle caratteristiche maggiormente apprezzate è la possibilità di garantire operatività e la disponibilità funzionale del dato, anche in modalità offline (desktop, web e mobile). La tecnologia prevede infatti una replica, di tutto o parte dei dati, delle funzionalità server e delle applicazioni, creando dei "package" auto-consistenti, residenti ad esempio sui dispositivi mobile o nelle postazioni di comando dei teatri operativi più o meno attrezzati. In presenza di nuova connettività avviene poi la sincronizzazione dei diversi package dislocati sul teatro operativo.

Le componenti Esri sopra descritte sono già integrate sui sistemi cloud, cogliendo e sfruttando tutti i vantaggi che questi ambienti offrono, tra cui la scalabilità, l'affidabilità e i servizi. Inoltre, già nel 2021 Esri ha rilasciato i primi *"Microservizi"* GIS di mapping e analisi. residenti su docker e containers orchestrati da Kubernetes.

MISURE BASATE SU LIDAR CON DEPOLARIZZAZIONE PER UNA MIGLIORE COMPRENSIONE DELLE CONDIZIONI ATMOSFERICHE

Studio della formazione delle nuvole con il Celiometro Vaisala CL61

EURELETTRONICA ICAS

Lo studio delle nubi e le loro proprietà rappresenta una difficoltà chiave nella comprensione del clima e della sua variabilità. La capacità di comprendere la formazione, la composizione e la fase delle nubi permetterebbe di migliorare sensibilmente le capacità di previsione modellistica sia a scopi operazionali che climatici a varie scale temporali. L'avvento dei satelliti ha permesso di ottenere informazioni molto utili e con una vasta copertura spaziale, ma senza un adeguato campionamento temporale a causa dagli alti periodi di rivoluzione dei sensori in orbita.

Con il celiometro di nuova generazione CL61, Vaisala ha introdotto per la prima volta in un sistema commerciale, una caratteristica innovativa: la misurazione della depolarizzazione. La radiazione emessa dal laser di un sistema Lidar risulta essere polarizzata linearmente. Il fascio laser inviato dall'apparato Lidar subisce un processo di depolarizzazione in seguito allo scattering (diffusione) da particelle non sferiche presenti in atmosfera. Le nuove capacità di misura della depolarizzazione, che sono state finora utilizzate e sfruttate solo nei Lidar disponibili in applicazioni di ricerca, consentono di differenziare fra precipitazioni liquide e solide, di rilevare polvere, sabbia e gli strati delle ceneri vulcaniche.

Il celiometro CL61 è uno strumento innovativo perché consente in maniera completamente automatica di misurare ed analizzare le proprietà delle particelle presenti lungo il profilo atmosferico, di monitorare la presenza delle nubi e di dare informazioni sulle loro caratteristiche. Il celiometro Vaisala CL61 è dotato di ottiche a lente singola che migliorano significativamente il rapporto segnale-rumore per fornire profili di retrodiffusione ad alta risoluzione.

Con funzionalità finora disponibili solo nei Lidar per applicazioni di ricerca, il CL61 ha un prezzo molto conveniente, è semplice da installare ed utilizzare, non necessitando di manutenzione nè di calibrazione. CL61 è l'unico prodotto nella sua categoria disponibile sul mercato per applicazione di monitoraggio non presidiato, in modo continuo ed in tutte le condizioni meteorologiche. Sin dagli anni 1980 Vaisala è stata pioniere nella tecnologia dei Celiometri Lidar e vi sono migliaia di unità di Celiometri Lidar Vaisala installate in più di 110 paesi.

Photo courtesy: ENEA

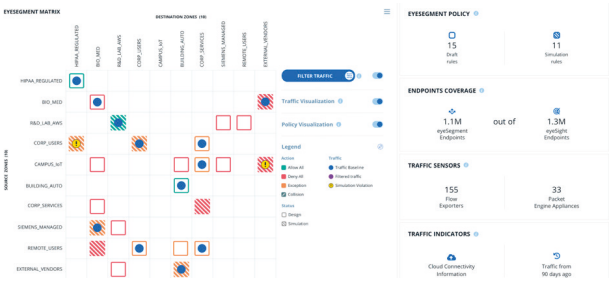
Vaisala Lidar Ceilometer CL61 Whitepaper | Vaisala

Un Celiometro CL61 è stato installato in Antartide a cura del Programma Nazionale Ricerche in Antartide (PNRA), per caratterizzare un'area come quella della base Mario Zucchelli situata sulle coste del mare di Ross dove è possibile osservare nubi a differenti fasi (solida, liquida, mista e sopraffusa). Il CL61 è un celiometro di ultima generazione e ha la peculiarità di fornire informazioni anche sulla fase delle particelle di acqua presenti lungo il profilo e di migliorare la comprensione della microfisica delle nubi polari. Fino ad oggi questo tipo di misura potevano essere ottenute solamente utilizzando strumentazione ben più costosa ma non utilizzabile in un ambiente cosi particolare come Mario Zucchelli. Lo strumento è stato montato durante la XXXVII campagna italiana in Antartide nel dicembre 2021, dando subito prova di essere uno strumento resistente ed adatto alle condizioni estreme resistendo senza problemi a differenti eventi di vento catabatico con venti che hanno superato 40 m/s. Lo strumento è tuttora acceso e funzionante anche dopo la chiusura della base avvenuta il 14 febbraio 2022. I dati trasmessi stanno mostrando ad una prima analisi la varietà e la coesistenza di fasi nelle nubi. In particolare, è stato possibile notare per la prima volta nell'area di MZS nubi liquide sopraffuse. "Il celiometro è uno strumento completamente automatico e necessita di pochissima manutenzione. Con l'aggiunta di queste nuove funzionalità sarà possibile effettuare un monitoraggio dell'atmosfera qualitativo, su lungo periodo, con una frequenza di campionamento molto alta e con costi relativamente bassi, contribuendo in maniera significativa alla comprensione della tipologia di nubi e del loro conseguente impatto sul clima antartico", spiega Paolo Grigioni, ricercatore ENEA del Laboratorio di Osservazioni e Misure per l'ambiente e il clima, nonché coordinatore dell'Osservatorio in Antartide.

FORESCOUT TECHNOLOGIES: VISIBILITÀ ESTESA DEI DISPOSITIVI

Difendi la tua Enterprise Of Things (EOT)

FORESCOUT TECHNOLOGIES



Forescout Technologies è l'azienda leader nel settore della visibilità e del controllo dei dispositivi. Per visibilità si intende sia la capacità di riconoscere il 100% dei dispositivi (risorse IoT incluse) connessi a reti, data center, cloud e ambienti OT sia la capacità di proteggere tali dispositivi mediante efficienti sistemi di controllo. La piattaforma di sicurezza unificata Forescout consente ad aziende e pubbliche amministrazioni di ottenere un quadro completo dei loro ambienti aziendali, garantendo un'operatività coordinata per ridurre il rischio informatico.

Le soluzioni Forescout permettono di individuare e di classificare, senza agent e in tempo reale, qualsiasi dispositivo con connessione IP valutandone il livello di sicurezza e facendo emergere eventuali condizioni di rischio per mancato rispetto delle normative di settore (cogenti e volontarie). Quest'anno si stima che il numero di dispositivi IP presenti sul mercato superi i 30 miliardi.

Le aziende riscontrano severe difficoltà non solo nell'individuare quanti dispositivi sono connessi alle loro reti, ma anche nel valutarne lo stato di sicurezza. Privi di un'adeguata protezione, questi dispositivi sono esposti a fattori di rischio informatico elevati. Forescout offre una soluzione atta a superare queste difficoltà, attuando un processo continuo di ricerca, classificazione e valutazione di ogni dispositivo con connessione IP che si aggancia alla rete aziendale. Negli ultimi vent'anni, il controllo degli accessi alla rete, il cosiddetto "NAC" (Network Access Control), si è rivelato uno strumento essenziale per implementare qualsiasi strategia di resilienza informatica in ambito aziendale. Il NAC è stato sviluppato per concedere o negare a un dispositivo l'autorizzazione ad accedere alla rete, garantendo un livello di protezione basico: stabilisce unicamente quali accessi autorizzare.

Tuttavia, la varietà e il volume dei dispositivi IoT (Internet of Things) e OT (Operational Technology) in circolazione sono talmente aumentati da esigere l'ampliamento delle capacità delle soluzioni NAC, affinché possano rilevare quantità di informazioni di sicurezza più dettagliate. Infatti, con il progressivo incremento della diversificazione dei dispositivi risulta decisivo l'ottenere una visibilità totale, una classificazione accurata e una applicazione corretta delle policy. È utile sottolineare come i potenziali criminali informatici riescano a spostarsi lateralmente all'interno delle reti aziendali non segmentate (Lateral spread), provocando gravi interruzioni delle normali attività nonché danni materiali e reputazionali. L'attacco hacker con ransomware WannaCry che colpì la compagnia di trasporti marittimi Maersk, per esempio, ne congelò l'attività finché la rete non fu bonificata dal malware. Se l'architettura della rete fosse stata in grado di limitare la mobilità del virus una volta penetrato, si sarebbe scongiurato il blocco.

Le reti non segmentate, in effetti, non assicurare il livello di granularità offerto dalle reti segmentate. I dispositivi IoT e OT che accedono a una rete che non è stata segmentata sono in grado di spostarsi lateralmente offuscando la visibilità così da creare punti ciechi utilizzabili dagli hacker.

Occorre sottolineare, inoltre, che la segmentazione della rete può essere dinamica. Se per tutti gli ambienti e i dispositivi si adottasse una strategia Zero Trust, definendo criteri di accesso diversi per un computer del front desk e il laptop del CEO, il rischio di attacco sarebbe automaticamente ridimensionato. Il controllo sulle reti e sull'ecosistema dei dispositivi diventa più complicato man mano che il numero di dispositivi IoT e OT aumenta. Per implementare una strategia di sicurezza efficace e ottenere visibilità e controllo totali, è necessario disporre della totalità dati relativi ai dispositivi connessi. Nel data center, nell'ambiente OT o nel cloud è preferibile consentire ai dispositivi accesso limitato anziché esteso all'intera rete.

In ambito aziendale la gestione di un numero crescente di vettori di attacco, rispettando tutti gli obblighi di conformità rappresenta un punto cruciale da affrontare per i responsabili della sicurezza. I miglioramenti apportati alle funzionalità di segmentazione sono stati proprio concepiti per consentire alle aziende di automatizzare il rilevamento e l'isolamento di possibili minacce alla sicurezza.

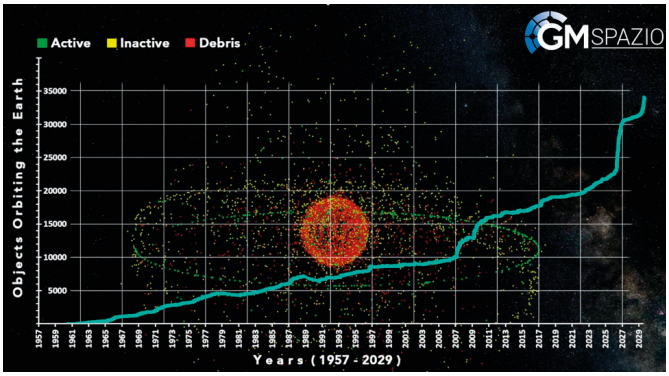
A partire dal 2020, a causa della pandemia da Covid-19, le minacce informatiche si sono acuite. La brusca transizione allo smart working e la necessità di predisporre l'accesso alle reti aziendali per i dipendenti che hanno iniziato a lavorare da remoto ha determinato un'impennata dell'utilizzo delle VPN. Poiché svariate applicazioni aziendali sono gestite centralmente on-premise, molti lavoratori necessitano di accedere alle reti, in particolare coloro che operano nel settore della pubblica amministrazione, in ambito sanitario

o in aziende di infrastrutture strategiche. Le aziende si affidano alle VPN per consentire agli utenti di collegarsi da remoto alla rete informatica aziendale tramite un canale protetto sotto forma di un tunnel criptato virtuale.
Le VPN, però, presentano un limite: preservano la sicurezza senza offrire altre funzionalità, come i controlli antimalware o le verifiche di conformità; pertanto, fungono unicamente da corsia di accesso preferenziale alle reti aziendali ma, in assenza di un'adeguata protezione, possono diventare facilmente bersagli per i criminali informatici.
Un altro aspetto su cui è importante porre l'accento è il fenomeno della convergenza delle reti IT e OT nelle reti aziendali. La convergenza è un elemento fondamentale all'interno del processo di trasformazione digitale. I benefici che ne derivano sono i seguenti: la manutenzione da remoto, la velocizzazione dei cicli di produzione, la riduzione dei tempi di approvvigionamento, l'acceleramento del passaggio dallo sviluppo di prototipi alla creazione del prodotto finale.
La connessione delle tecnologie IT e OT, tuttavia, comporta anche alcuni svantaggi: un maggiore numero di dispositivi connessi significa anche una moltiplicazione dei punti di accesso alla rete e, quindi, di potenziali vettori di attacco informatico. Forescout, attualmente, è impegnata nell'avviamento di progetti tesi a risolvere le problematiche appena descritte.
Sotto il profilo della visibilità sui dispositivi della rete (dispositivi personali, IT, OT o presenti su base permanente) i risultati emersi da una ricerca condotta nel 2021 da Forescout indicano che l'85% dei responsabili IT concorda sul fatto che l'assenza di visibilità rappresenta il punto debole di qualsiasi infrastruttura di sicurezza e che le aziende che si attivano per ottenere una visibilità completa sulla rete scoprono, in media, il 30% in più di dispositivi rispetto al numero previsto inizialmente. La soddisfazione del requisito della visibilità consente di raggruppare tutti i dispositivi e gli utenti attraverso un solo sistema di gestione, applicando policy di sicurezza a tappeto o singolarmente. È possibile, per esempio, autorizzare l'accesso alla rete aziendale a un laptop, sottoponendo istantaneamente a quarantena eventuali connessioni non conformi. E tramite una procedura di segmentazione dei dispositivi connessi alla rete si può, inoltre, contenere la diffusione degli attacchi impedendo che essi infettino l'intera rete.
Forescout aiuta i propri clienti aventi reti estese a ottenere visibilità su tutti i dispositivi, a prescindere dal fatto che questi ultimi siano connessi alla rete, che siano preposti all'automazione degli edifici o che operino in ambienti OT, cloud o in data center. Quanto illustrato poggia su uno specifico modello di sicurezza, il cosiddetto modello "Zero Trust": ogni richiesta di accesso alla rete deve essere verificata e autorizzata. La protezione di ambienti sempre più eterogenei e frammentati implica il superamento dei tradizionali metodi di autenticazione basati sulla sicurezza perimetrale, perché le minacce informatiche possono essere sia esogene sia endogene.
Il modello "Zero Trust" dovrebbe essere applicato all'interno di qualsiasi infrastruttura di sicurezza, dato che la visibilità rappresenta il criterio cardine di qualsiasi sistema di sicurezza.
Al fine di mettere in sicurezza i dispositivi IoT e OT non protetti Forescout ha lanciato "eyeSegmet", una soluzione che consente di edificare una efficace architettura di segmentazione della rete raggruppando utenti e dispositivi per tipo e contesto aziendale in zone intelligenti e, allo stesso tempo, limitando l'accesso alla rete unicamente alle risorse ritenute necessarie a fini lavorativi.
Questa soluzione sfrutta il livello elevato di visibilità raggiunto sui dispositivi e i dati contestuali -forniti da Forescout eyeSight mediante aggiornamenti in tempo reale- evidenziando i flussi di traffico e le dipendenze che intercorrono tra utenti, applicazioni, servizi e dispositivi.
Forescout eyeSegment, dunque, aiuta a progettare, creare e perfezionare efficaci criteri di segmentazione (simulabili previa attivazione) basati su una tassonomia aziendale che, però, può essere applicata a tutte le tecnologie di base esistenti.
Nello specifico, un criterio di segmentazione consiste in un insieme di regole stabilite per autorizzare in toto, bloccare in toto o autorizzare parzialmente il traffico dei dati tra specifiche zone di partenza e arrivo. Sono considerate "zone" anche singoli indirizzi IP e oggetti Forescout creati dalla segmentazione e appartenenti a gruppi. Ogni zona di segmentazione può essere impostata come zona di partenza e/o zona di arrivo.
Mediante un'unica console è possibile creare criteri di segmentazione che negano o autorizzano esplicitamente il traffico in transito attraverso domini di rete e tecnologie diverse. È importante sottolineare, infine, quanto segue: è autorizzato il traffico proveniente da qualsiasi zona di partenza e diretto a qualsiasi zona di arrivo, perché definendo criteri ed eccezioni, è possibile stabilire il traffico autorizzato e quello negato così da permettere agli utenti di specificare azioni diverse per singoli sottogruppi e servizi.

CAPIRE LO SPAZIO E SAPERLO GESTIRE: GMSPAZIO, LAVORARE NEL PRESENTE PER PROTEGGERE IL FUTURO

SDA, SSA e SST per la salvaguardia di persone e risorse

GMSPAZIO



Negli ultimi sessant'anni sono stati collocati in orbite vicine e lontane alla Terra oltre 10.000 oggetti spaziali ed il loro numero crescerà esponenzialmente alla luce dei progressi tecnologici che hanno miniaturizzato le piattaforme satellitari e reso riutilizzabili i lanciatori. Un crescendo incontenibile ma disordinato perché la tecnologia spaziale si è sviluppata più rapidamente della regolamentazione dell'uso dello spazio, soprattutto riguardo la gestione delle orbite e dei detriti spaziali, questi ultimi potenziali inibitori di futuri accessi allo spazio, capaci di limitare l'espansione del genere umano al di fuori del pianeta Terra.

Un'evoluzione repentina ma potenzialmente drammatica che potrebbe saturare lo spazio vicino con oggetti in orbite incontrollate percorse a velocità di 7 km al secondo, in grado di provocare danni inimmaginabili a tutte le piattaforme spaziali dedicate alla TV, alle telecomunicazioni, alla navigazione assistita ed alla tutela dell'ambiente.

Lo spazio è un luogo in cui il genere umano vive, lavora e combatte, considerato il numero crescente di attori istituzionali e commerciali in grado di accedere allo spazio e interessati ad utilizzarlo, con una crescente concorrenza volta ad ottenere il primato nel suo sfruttamento.

Dobbiamo diventare capaci di gestire al meglio questa risorsa: identificare chi lo popola, capire come si modifica e salvare le nostre risorse strategiche in orbita, considerando anche che alcune delle attività più importanti nella pianificazione e nell'esecuzione di operazioni militari si svolgono al giorno d'oggi nello spazio stesso.

Da quando è nata, GMSPAZIO si occupa di modellazione e simulazione di ambienti complessi e come naturale evoluzione del tema, dal 2010 si occupa dello Space Domain Awareness (SDA) e delle sue declinazioni: Space Situational Awareness (SSA) e Space Surveillance and Tracking (SST), indispensabili a localizzare, tracciare, identificare e valutare le minacce che incidono sulla sicurezza degli asset in orbita e sulle loro prestazioni, per contribuire alla salvaguardia, a breve e lungo termine, di infrastrutture, mezzi e servizi spaziali di importanza strategica per le nazioni coinvolte.

Una sfida complessa, ma necessaria per la protezione del nostro futuro e degli investimenti fatti in questa direzione.

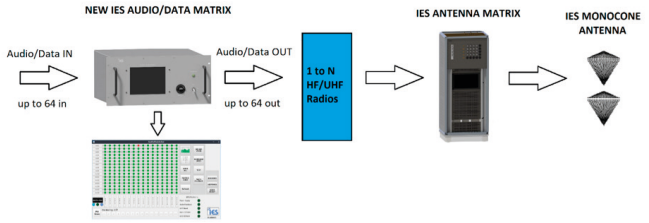
Conoscere gli oggetti spaziali, identificarli, stabilirne le orbite, misurarne le operazioni e prevedere le loro future posizioni nello spazio e nel tempo sono azioni basilari per acquisire, valutare e calcolare tutte le informazioni inerenti l'ambiente spaziale. La prima esigenza è quindi la necessità di monitorare in modo preciso gli oggetti orbitanti per valutare l'opportunità di effettuare manovre di messa in sicurezza oppure evitare le stesse risparmiando il carburante a bordo ed allungando di conseguenza la vita operativa della missione a cui appartengono. Senza dimenticare però che è necessario operare anche per contrastare la proliferazione di detriti spaziali, tenendo traccia degli effetti di collisioni o esplosioni, così da avere una mappa aggiornata in tempo reale dei potenziali rischi durante i lanci sempre più frequenti di vettori spaziali e sorvegliare i rientri non controllati in atmosfera.

Noi di GMSPAZIO siamo al posto giusto al momento giusto per supportare i nostri interlocutori nella gestione di situazioni complesse allo scopo di garantire la massima efficienza dei loro sistemi ed al contempo tutelare la sicurezza della comunità contro i potenziali rischi derivati dall'uso incontrollato delle risorse spaziali.

SISTEMI DI COMUNICAZIONE RESILIENTI AD ELEVATA AFFIDABILITÀ

HF 4th Generation Communication System

IES



Allo stato attuale le forze militari fanno affidamento su comunicazioni satellitari tattiche che consentono di ottenere ampia copertura sul territorio, flessibilità, buona velocità di trasmissione dati, e capacità di comunicazione senza linea di vista (BLOS - Beyond-Line-of-Sight). Tuttavia, questo può essere oggetto di attacchi elettronici che rendono il nodo satellitare un "single point of failure" del sistema, mettendo a rischio l'intera missione.

Il Dipartimento per la sicurezza nazionale statunitense ha investigato e dimostrato la possibilità di realizzare punti morti in modo artificioso: i transreceiver dei satelliti SATCOM sono stati accecati focalizzando il plasma e campo magnetico radiato dalla massa coronale del sole verso le loro antenne. Con il programma SHARES (SHAred RESources HF Radio Program), l'agenzia statunitense per la sicurezza delle infrastrutture e cybersecurity risponde già a questo tipo di minaccia, proponendo la banda HF non solo come soluzione di backup alle comunicazioni satellitari, ma anche come infrastruttura imprescindibile delle comunicazioni tattiche, grazie alla loro indiscussa affidabilità e resilienza in condizioni operative. I sistemi di comunicazione basati su onde HF (1.5-30MHz) sono noti da tempo per avere maggiore resilienza agli attacchi grazie alla possibilità di creare una rete distribuita di nodi formata dalle unità stesse sul territorio.

Negli ultimi anni, gli enti di standardizzazione militare hanno definito un nuovo standard per comunicazioni HF (MIL-STD-188-110 vers.D, Dic. 2017) a larga banda, che consente un trasferimento dati fino a 240kbps.

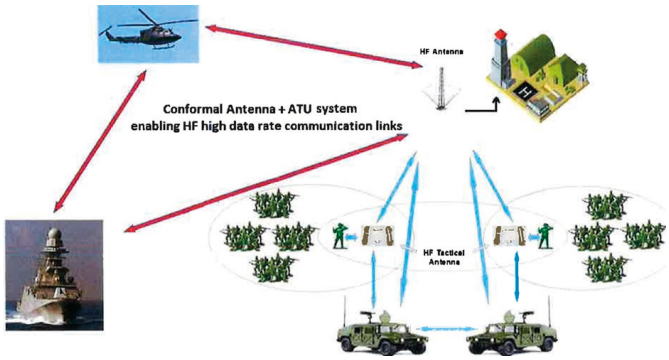
La IES ha realizzato sistemi di telecomunicazione completi offrendo la possibilità di sfruttare appieno le potenzialità dell'HF introducendo una linea di prodotti unici nel loro genere e compatibili con le nuove forme d'onda HF e con i relativi link tattici. Ne è un esempio la nuova matrice audio/dati espandibile fino a 64 canali di ingresso/uscita che è già compatibile con i nuovi standard e perfettamente integrabile nel potenziamento di sistemi preesistenti. Per quanto riguarda la catena di condizionamento dei segnali RF di potenza la IES ha realizzato una nuova matrice antenna ed un'antenna a larga banda (monocono invertito) con funzionalità di monitoraggio dei parametri strutturali della stessa per una efficiente gestione della manutenzione preventiva rappresenta lo stato dell'arte della tecnologia.

I prodotti IES si collocano nel cuore di ogni sistema di comunicazione sia esso SSSB (Ship-Shore-Ship Buffer) che BRASS (Broadcast, maritime Rear link And Ship to Shore).

Parallelamente a ciò, l'evoluzione dell'attuale sistema BRASS (Broadcast, maritime rear link and ship-to-shore) ampiamente diffuso nelle nazioni NATO, mediante l'introduzione del nuovo sistema BRE1TA (BRASS Enhancements Increment 1 Target Architecture) a definizione dei nuovi standard, prevede l'implementazione di sistemi software che consentono lo sviluppo delle capacità di comunicazione BLOS (Beyond line of sight) e quindi, conseguentemente, la possibilità di utilizzare servizi IP tramite HF (chat, email, instant messaging).

Ma il sistema BRE1TA, pur rappresentando un significativo passo in avanti che consente di sfruttare nuove tecnologie, rispetto al predecessore sistema BRASS, presenta tuttavia delle limitazioni legate soprattutto alla velocità di trasmissione dei dati tramite HF di precedente generazione.

Allo stato attuale coniugando i nuovi sistemi radio a larga banda con sistemi d'antenna WBHF (wide band HF) è possibile pensare a sistemi più evoluti che permetterebbero l'introduzione di ulteriori funzionalità quali, ad esempio, il trasferimento di flussi video all'interno di architetture moderne come il BRE1TA e non solo. Per questo la IES propone oltre all'utilizzo di radio SDR di quarta generazione e allo sviluppo di moderni sistemi d'antenna conformi alle superfici dei mezzi, l'impiego di nuovi sistemi di filtraggio che consentono di supportare il frequency hopping.



REALISMO E ACCURATEZZA NELLA SIMULAZIONE DELLO SPETTRO ELETTROMAGNETICO

Soluzioni di analisi e simulazione

KEYSIGHT TECHNOLOGIES

Lo Spazio e la Difesa sono la spina dorsale della moderna innovazione commerciale e viceversa.
Internet, le comunicazioni wireless, i satelliti, lo spazio, la navigazione e l'elettrificazione sono in continua evoluzione. Spingere i confini dei limiti tecnici richiede una combinazione di conoscenza approfondita e immaginazione per esplorare nuove possibilità. Keysight contribuisce fornendo soluzioni con innovazioni tecnologiche all'avanguardia in ambito Spazio e Difesa con hardware e software COTS scalabili e ad alte prestazioni.
Vediamo qualche esempio in ambito applicativo.

LA SFIDA DELLA GUERRA ELETTRONICA

L'evoluzione di radar, guerra elettronica (EW) e contromisure richiedono la generazione e l'analisi di segnali complessi per la simulazione e il test. Di pari passo evolvono le sfide nel rilevare, evitare e contrastare gli attacchi con l'avanzare della tecnologia. In tutti i casi, il test dei sistemi odierni beneficia di apparecchiature di misura ad alte prestazioni: generatori di segnali analogici e vettoriali, analizzatori di spettro, analizzatori di segnali vettoriali, analizzatori di reti vettoriali e altro ancora. Dalle simulazioni di un segnale in arrivo con più emettitori, al test di componenti di precisione in un ricevitore, le soluzioni Keysight sono pronte per gestire la complessità delle applicazioni di test di guerra elettronica (EW).

SIMULAZIONE DINAMICA DI MINACCE AD ALTA DENSITÀ

Le nostre soluzioni vengono costantemente aggiornate a minacce nuove e complesse con la simulazione dei segnali, creando scenari di guerra elettronica (EW) complessi, con una elevata densità di impulsi e con la simulazione simultanea sia dell'angolo di arrivo (AoA) che della cinematica (piattaforme mobili) grazie a generatori di segnali agili e coerenti. La soluzione Keysight è una combinazione di sorgenti di segnale, hardware e software di calibrazione e software applicativo per la generazione di scenari predefiniti o dinamici in grado di simulare un campo di battaglia elettronico con migliaia di emettitori.

REGISTRAZIONE E ANALISI CONTINUA DEI SEGNALI

La verifica accurata dei dati di ingresso e uscita del sistema sottoposto a test è fondamentale per validarne la funzione e le prestazioni. La maggior parte dell'attuale hardware di

analisi ha capacità limitate, il che si traduce nella verifica parziale dei segnali, utilizzando analizzatori di spettro o oscilloscopi di fascia alta. L'acquisizione e la registrazione continua dei segnali di interesse per tutta la durata di uno scenario di prova è necessaria per verificare il corretto funzionamento. Keysight offre soluzioni completamente integrate, multicanale, multibanda, con misurazione in tempo reale e riconoscimento degli impulsi, nonché ore di archiviazione dei dati RF registrati. I casi d'uso includono il collaudo dei sistemi di attacco elettronico e la verifica dei sistemi di simulazione delle minacce.

SISTEMI DI COMUNICAZIONE MILITARI

Le comunicazioni militari (MilCom) richiedono prestazioni, interoperabilità e affidabilità in reti che vanno da una copertura ad hoc e locale a un'area più ampia con il supporto dell'infrastruttura cellulare. Molte soluzioni MilCom devono supportare simultaneamente apparecchiature per comunicazioni militari consolidate e tecnologie più recenti. Per fornire una maggiore consapevolezza della situazione, per le MilCom si sfruttano sempre di più tecnologie commerciali come Long Term Evolution (LTE), di quinta generazione (5G) e reti locali wireless (WLAN). Le reti MilCom realizzano anche i vantaggi derivanti dall'adozione di formati di modulazione digitale più recenti. Le soluzioni di misura devono essere in grado di testare tutti gli aspetti di queste radio versatili man mano che si evolvono con la tecnologia delle comunicazioni. Il nostro approccio di test scalabile e flessibile consente di ridurre al minimo il trasferimento di proprietà intellettuale (IP), accelerare i tempi di produzione, ridurre i costi di ingegneria del test e migliorare la correlazione tra le misure.

La nostra missione: garantire maggiore realismo per una maggiore affidabilità. Affidati a Keysight - soluzioni e servizi – l'evoluzione del tuo laboratorio.
Scopri di più: https://connectlp.keysight.com/difesa

CONOSCERE [È] PROTEGGERE: LA CULTURA DELLA SICUREZZA PER AFFRONTARE LE MINACCE DEL NOSTRO TEMPO

Al via la Cyber & Security Academy di Leonardo

LEONARDO

Agli inizi del 2022 è nata la nuova Cyber & Security Academy di Leonardo, polo di alta formazione realizzato dall'azienda per garantire a istituzioni, infrastrutture critiche e imprese le competenze e le capacità necessarie per supportare la transizione digitale e fronteggiare le minacce alla sicurezza nazionale. Con sede principale a Genova e la capacità di erogare corsi in Italia e all'estero attraverso diverse strutture sul territorio, la Cyber & Security Academy ha l'obiettivo di rendere la sicurezza, cyber e non solo, un tema sistemico di tutte le organizzazioni. Cuore tecnologico dell'Academy sono le piattaforme Cyber Range e Cyber Trainer. Progettate secondo i principi della gamification, sfruttando cioè meccanismi simili a quelli dei giochi, simulano scenari operativi immersivi complessi in cui mettere in pratica, in gruppo o individualmente, le conoscenze acquisite grazie alla creazione di gemelli digitali (digital twin) di reti, sistemi e applicazioni da proteggere, oltre che di minacce e tool per attacco e difesa. L'Academy propone un'offerta formativa complementare rispetto ai corsi universitari, ai master post-laurea e alle certificazioni specialistiche, che si rivolge a tutti i principali attori coinvolti nella gestione della sicurezza nazionale. Inoltre prevede un approccio alla formazione della sicurezza intesa in senso completo e convergente. Un approccio che coinvolge sia tecnologie, processi e normative, sia il fattore umano, essenziale per poter gestire in modo adeguato le crisi derivanti da attacchi e incidenti con impatti su larga scala. In questo contesto, la Leonardo Cyber & Security Academy si fonda su tre elementi portanti:

- **Cultura della Sicurezza:** la Cyber & Security Academy di Leonardo promuove la Cultura della Sicurezza attraverso un'offerta formativa di alto profilo, proponendo un approccio multilaterale al tema della sicurezza per garantire percorsi formativi diversificati in base al contesto operativo, basati sulle competenze maturate dai team di sicurezza di Leonardo nell'ambito di domini critici.
- **Educare e Istruire**, la Cyber & Security Academy coniuga due approcci complementari: l'istruzione, per l'acquisizione di informazioni, e l'educazione, per valorizzare le persone in termini di capacità di collaborazione e risoluzione dei problemi. Questa complementarietà è fondamentale nell'ambito della sicurezza multi-dominio, dove è strategico saper coniugare competenze tecniche con comportamenti cooperanti in un'ottica di efficienza ed efficacia dell'attività formativa
- **Percorsi Formativi Immersivi:** attraverso l'utilizzo di piattaforme proprietarie di addestramento basate sulla simulazione di contesti operativi reali, l'Academy offre inoltre percorsi formativi capaci di conformarsi esattamente alla realtà di ciascuna organizzazione.

Il catalogo dell'Academy è strutturato attraverso **percorsi di apprendimento** (Learning Paths) che identificano i diversi domini di specializzazione che i discenti possono intraprendere **nell'ambito dei temi più attuali della global security** in termini tecnologici, normativi e di approccio metodologico. Questi percorsi di apprendimento includono anche un'ampia gamma di corsi su aree tematiche meno verticali che spaziano dallo sviluppo dei soft skill all'acquisizione di competenze sulle tecnologie più utilizzate nell'ambito della sicurezza. L'Academy eroga inoltre corsi di **Cyber Security Awareness** con l'obiettivo di fornire una conoscenza basilare dei concetti e delle best practices afferenti alla sicurezza informatica destinati ad utenti non esperti di Cyber Security. Completano il catalogo corsi dell'Academy le attività di **Cyber Exercise** e di **White Phishing**, che consistono rispettivamente in esercitazioni finalizzate a testare la preparazione dei partecipanti in merito alle procedure di sicurezza della propria organizzazione e nell'invio di campagne di phishing simulate con l'obiettivo di misurare il livello di consapevolezza dei dipendenti rispetto alle minacce cibernetiche veicolate via e-mail.

L'Academy si avvale di un corpo docente costituito da esperti in grado di individuare i contenuti e gli strumenti formativi più adeguati alle esigenze degli utenti (lezioni frontali, in presenza e digitali, video corsi, pillole formative).

L'Academy dispone anche di un **Certification & Testing Center** funzionale al conseguimento di certificazioni delle principali aziende di hardware e software, e in prospettiva, anche di prodotti sviluppati da Leonardo.

SPACE SITUATIONAL AWARENESS (SSA) PER ATTIVITÀ SPAZIALI SICURE, STABILI E SOSTENIBILI

Il ruolo di Leonardo

LEONARDO

Rischi e minacce spaziali sono in costante aumento: se trascurati, lo spazio diverrebbe rapidamente inospitale per le operazioni satellitari.

- I detriti spaziali, per lo più derivanti da oggetti di fabbricazione umana, restano in orbita anche dopo il completamento delle missioni che li hanno originati;
- alcune azioni sono condotte per il danneggiamento dei satelliti, ad esempio l'uso di navicelle per avvicinarsi al satellite obiettivo e renderlo non operativo mediante mezzi cinetici o elettronici;
- I satelliti attivi sono sempre più numerosi: alcune compagnie realizzeranno costellazioni di migliaia di satelliti in LEO (Low Earth Orbit) per le comunicazioni a larga banda;

La Space Situational Awareness (SSA) è una tematica di interesse duale. In ambito civile, si applica al tracciamento di oggetti, corpi naturali e allo studio del tempo meteorologico spaziale; in ambito militare, identificando rischi e minacce nello spazio, dallo spazio e verso lo spazio. In particolare, con Space Surveillance and Tracking (SST) si intende la capacità di rivelare e predire il movimento degli oggetti in orbita, contribuendo alla prevenzione delle collisioni e alla pianificazione delle manovre satellitari.

Leonardo è partner chiave del MoD Italiano per lo sviluppo delle capacità SSA nazionali, prevalentemente nel segmento terrestre in quanto sede delle infrastrutture, del Comando e Controllo (C2) e punto di osservazione ottimale dello spazio. In particolare Leonardo sin dal principio supporta lo sviluppo della capacità SST ed è leader nazionale per la fornitura dei servizi Fragmentation, Re-entry e Collision Avoidance nel contesto SST.

Leonardo contribuisce inoltre alla costruzione di una capacità SSA militare autonoma a livello europeo, adeguando il proprio piano di sviluppo industriale, conforme alle priorità nazionali, agli orientamenti europei espressi negli ambiti EDIDP (European Defence Industrial Development Programme), EDF (European Defence Fund) ed EU-SST, in cui Leonardo occupa una posizione di primo piano.

- **EU-SST:** Leonardo è il partner industriale nazionale per l'implementazione dei servizi SST (a partire da Italian Space Operation Centre e sensori terrestri);

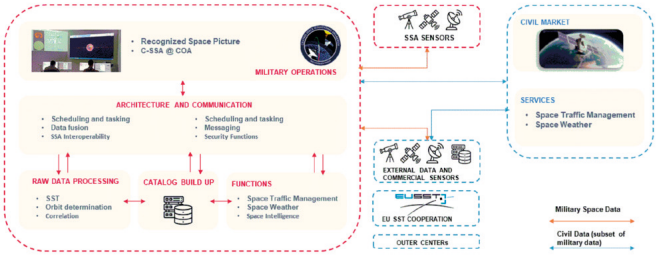


Fig. 1: Space Situational Awareness - una capacità duale.

- **EDIDP:** Leonardo è il coordinatore del progetto INTEGRAL finalizzato alla realizzazione del C2 per la capacità SSA e partner chiave del progetto SAURON per la tecnologia radar;
- **EDA:** Leonardo guida il consorzio europeo per 'Study for a Defense Approach to Space Traffic Management and Coordination (STM) and Enabling Space-based Military Space Situational Awareness (SSA) capabilities'.

L'approccio duale adottato da Leonardo per l'implementazione della capacità SSA è riportato in Figura 1, a dimostrazione dell'interoperabilità tra i domini militare e civile.

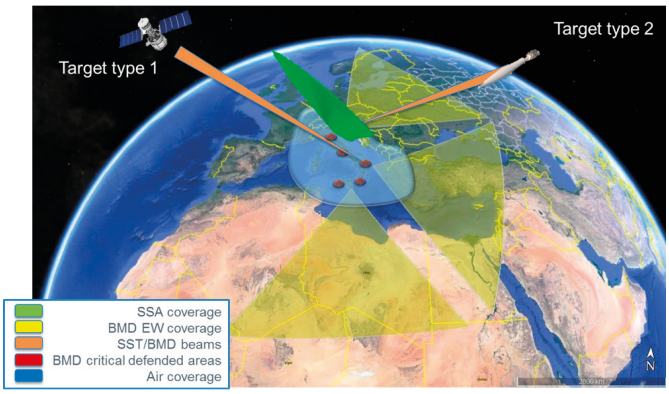


Fig. 2: Approccio Leonardo per Integrated Air Missile and Space Defence.

DIGITAL TWIN: STATO E POSSIBILI MODI DI SVILUPPO DELLA TECNOLOGIA

La visione di Leonardo

LEONARDO

Un gemello digitale (Digital Twin) è una rappresentazione virtuale di un oggetto o di un sistema che viene aggiornato da dati in tempo reale e utilizza la simulazione, l'apprendimento automatico e il ragionamento per aiutare il processo decisionale. Un gemello digitale funge da controparte n tempo reale di un oggetto o processo fisico. Sebbene il concetto abbia avuto origine nel 2002, la prima definizione pratica ha avuto origine dalla NASA nel 2010, per migliorare la simulazione del modello fisico di veicoli spaziali. I gemelli digitali sono il risultato del miglioramento continuo nelle attività di progettazione e ingegneria di prodotto.

I disegni dei prodotti e le specifiche ingegneristiche sono passati dalla progettazione fatta a mano alla progettazione assistita da computer, per arrivare all'ingegneria dei sistemi basata su modelli.

Il concetto di gemello digitale si compone di tre parti distinte:

- il prodotto fisico,
- il prodotto digitale\virtuale,
- collegamenti tra i due prodotti.

Esistono diversi tipi di gemello digitale: **prototipo di gemello digitale (PGD)**: il PGD consiste in progetti, analisi e processi per realizzare un prodotto fisico. Il PGD esiste prima che ci sia un prodotto fisico.

- **l'istanza del gemello digitale (IGD):** il IGD è il gemello digitale di ogni singola istanza del prodotto una volta prodotto.
- **il digital twin aggregate (DTA):** il DTA è l'aggregazione di IGD i cui dati e informazioni possono essere utilizzati per interrogazioni sul prodotto fisico, prognosi e apprendimento.

il Digital Twin può essere suddiviso in tre sottocategorie in base al diverso livello di integrazione, ovvero il diverso grado di flusso di dati e informazioni che può verificarsi tra la parte fisica e la copia digitale:

- Modello Digitale (DD),
- Ombra digitale (OD)
- Gemello digitale.

Un gemello digitale è un modello virtuale progettato per riflettere accuratamente un oggetto fisico. L'oggetto in studio, ad esempio una turbina, è dotato di vari sensori relativi ad aree vitali di funzionalità. Questi sensori producono dati su diversi aspetti delle prestazioni dell'oggetto fisico, come la produzione di energia, la temperatura, le condizioni meteorologiche e altro ancora. Questi dati vengono quindi inoltrati a un sistema di elaborazione e applicati alla copia digitale. Una volta dotato di tali dati, il modello virtuale può essere utilizzato per eseguire simulazioni, studiare problemi di prestazioni e generare possibili miglioramenti, con l'obiettivo di generare informazioni che possono quindi essere riapplicate all'oggetto fisico originale. La differenza tra gemello digitale e simulazione è in gran parte una questione di scala: mentre una simulazione studia in genere un processo particolare, un gemello digitale può eseguire un numero qualsiasi di simulazioni utili per studiare più processi. Le differenze non finiscono qui. Ad esempio, le simulazioni di solito non traggono vantaggio dall'avere dati in tempo reale. Invece i gemelli digitali sono progettati attorno a un flusso di informazioni bidirezionale che si verifica prima quando i sensori di oggetti forniscono dati rilevanti al processore di sistema e poi si ripresenta quando le informazioni dettagliate create dal processore vengono condivise con l'oggetto di origine. Poiché hanno dati migliori e costantemente aggiornati relativi a un'ampia gamma di aree, combinati con la potenza di calcolo aggiuntiva che accompagna un ambiente virtuale, i gemelli digitali sono in grado di studiare più problemi da punti di vista molto più vantaggiosi rispetto alle simulazioni standard, con un maggiore potenziale di miglioramento per prodotti e processi. In Italia, Leonardo si sta ritagliando un ruolo guida i grazie ai Leonardo Labs, una rete internazionale di laboratori proprietari dedicati alla ricerca e all'innovazione tecnologica, che lavorano soprattutto sulla progettazione di un framework per digital twin per la fase di progettazione (digital twin prototype in cui il modello è disponibile prima della costruzione del sistema reale) e della sua interazione col mondo reale. Molti oggi confondono il Digital Twin con la simulazione avanzata ma le differenze sono enormi, di scala e di connessione. La simulazione è molto più puntuale sui componenti mentre il Digital Twin utilizza una scala di sistema generale e soprattutto si serve di una connessione continua e costante con l'oggetto reale. Gestire una quantità di dati così mostruosa richiede una capacità di calcolo importante e questa è l'anima del Digital Twin che per noi è basata sul nostro super-calcolatore Davinci-1.

UN APPROCCIO SOFTWARE-CONNECTED PER LA DIGITAL TRANSFORMATION NEL TEST AND EVALUATION

NATIONAL INSTRUMENTS ITALY

Oggi le operazioni nello spettro elettromagnetico (Electro-Magnetic Spectrum Operations, EMSO) richiedono la rapida evoluzione dei principi e delle architetture di Test & Evaluation (T&E) per far fronte alle sfide ingegneristiche e operative durante tutto il ciclo di vita di sistema, dei moderni sistemi radar, di guerra elettronica (EW) e comunicazione, navigazione e sorveglianza (CNS), Figura 1.

Tutti i sistemi operanti nel moderno EMS si basano sempre di più su:

- funzionalità basate su SW, che consentono agilità, adattabilità, cognizione e "intelligenza artificiale";
- suite di sensori federati, multidominio e system-of-systems (SoS);
- e cyberspace.

Queste sfide vengono affrontate dalla Digital Transformation delle capacità di T&E, che offre agli ingegneri di verifica e validazione un'infrastruttura agile e altamente programmabile per modellare e generare gli stimoli per i sistemi sotto test.

Tuttavia, questa trasformazione richiede un approccio integrato e interfunzionale per migliorare l'utilizzo e l'efficienza delle risorse T&E in tutte le fasi del ciclo di vita (System Life Cycle, SLC), ridurre il costo totale del test; ed accelerare il time-to-market, introducendo il concetto di Software e Hardware in the Loop (SiL/HiL) in tutte le fasi del SLC ed in qualsiasi ambiente di prova (ufficio, laboratorio, banchi prova, camere anecoiche, strutture di integrazione, test ranges all'aperto).

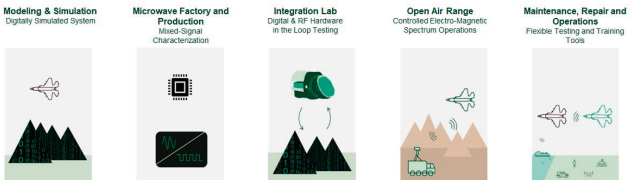


Fig. 1 - T&E sul ciclo di vita di sistema

Il prerequisito per la modellazione e la simulazione, è una piattaforma HW flessibile, che soddisfi i requisiti di:

- MODULARITÀ per aggiungere/rimuovere funzioni e capacità in base all'attuale "punto di vista" sul sistema;
- SCALABILITÀ in termini di numero di canali, risorse computazionali, bande di frequenza;
- FLESSIBILITA' in termini di funzioni da ospitare e possibilità di essere riprogrammata (software-defined) e collegate ad altri sistemi e/o strumenti per la condivisione e il controllo dei dati. Deve essere facile da usare per analisti, sviluppatori SW e ingegneri di test, e deve soddisfare i requisiti derivanti dalle tipiche applicazioni EMSO come: banda fuori frequenza; ampia larghezza di banda istantanea; decine di canali coerenti in fase; gamma dinamica per far fronte a bersagli con RCS (Radar Cross Section) variabile a seconda del tipo di bersaglio da emulare.

I requisiti di modularità HW, programmabilità, scalabilità, affidabilità, risorse computazionali, connettività, storage di memoria, ecc., sono le caratteristiche chiave di NI Vector Signal Transceiver (VST), e della piattaforma NI PXI. Il VST, Figura 2, è uno strumento calibrato modulare e software-defined che si adatta molto bene ai requisiti dei moderni sistemi T&E, come la latenza I/O (<1us) e l'ampia larghezza di banda istantanea (1 GHz). La disponibilità di un FPGA aperto all'utente, rende lo strumento flessibile per ospitare qualsiasi applicazione di modellazione, simulazione, elaborazione e controllo in tempo reale.

Nella stessa figura è riportato un semplice esempio di Radar Target Generator (RTG) con quattro target indipendenti in frequenza, guadagno e ritardo temporale. La modularità della piattaforma PXI permette di aggiungere, al VST, diverse risorse di processing, basate su FPGA e/o CPU, per aumentare le capacità di calcolo e simulare diversi tipi di scenario con un altissimo levelli di affidabilità.

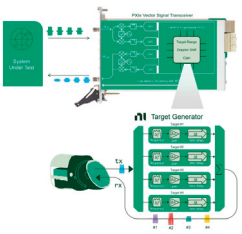


Fig. 2 – Radar Target Generator basato su NI Vector Signal Transceiver

Inoltre, la capacità di sincronizzazione spinta degli ADC, DAC ed oscillatori, basata sulla technologia NI-TClk, Figura 3, e la capacità di trasmissione dei dati ad elevato throughput della piattaforma NI PXI, sono fattori chiave per la creazione di un sistema ricevitore e trasmettitore multicanale allineato in fase per supportare le nuove sfide dei sistemi di T&E in ambito Radar, EW, e CNS, che operano nel moderno spettro elettromagnetico.

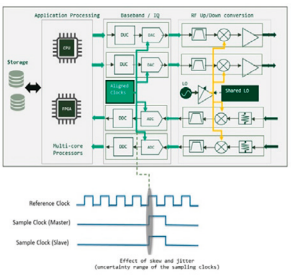


Fig. 3 - Block Diagram of a Multichannel Phase Aligned Transceiver (2 Channel Transceiver)

RIDURRE IL RISCHIO NELLE APPLICAZIONI DI TEST AEROSPAZIALI CON PIATTAFORME APERTE

Come sfruttare il COTS per ridurre il rischio e migliorare il costo complessivo del Sistema

NATIONAL INSTRUMENTS ITALY

I responsabili dei programmi aerospaziali si preoccupano di soddisfare i requisiti dei clienti e di prevenire eventuali perdite di qualità, piuttosto che del funzionamento interno della loro architettura di test. I budget al di fuori di un programma sono rari e la necessità di un aggiornamento si presenta di solito nel bel mezzo del programma stesso, quando si è più avversi al rischio. Fattori come la progettazione del sistema di test, il cablaggio punto-punto e la costruzione di adattatori di test sono essenziali per creare un sistema di test funzionante, ma non contribuiscono necessariamente ad aumentare la qualità del prodotto.

L'hardware rappresenta in genere meno di un quarto del costo totale, mentre la manodopera per la progettazione e la costruzione incide maggiormente sul budget e sulle tempistiche. Sulla base di dati tipici, si possono stimare da 800 a 1.000 dollari per ogni pin di I/O con una tempistica di 8-12 mesi, a seconda delle dimensioni del sistema.

Caratteristiche comuni dei sistemi di test LRU

Un sistema di test LRU di base consiste in un'unità sottoposta a test (UUT) interfacciata a un'interconnessione di massa che è collegata ad I/O di simulazione gestiti da un applicativo di test che realizza la simulazione del velivolo.

È possibile personalizzare questa configurazione di base per includere l'aggiunta del condizionamento del segnale per la simulazione dei sensori e dei carichi specifici che devono essere pilotati dall'UUT, nonché l'inserimento di guasti per il test del software. Ulteriori personalizzazioni possono comprendere una breakout box per l'inserimento manuale dei guasti, l'iniezione e il reindirizzamento dei segnali, nonché linee di rilevamento per sapere esattamente cosa vede la LRU durante tutte le fasi del test. Le linee di rilevamento possono rendere necessaria una misura di tipo strumentale.

Se si considera il parametro standard del settore di tre minuti per terminazione del filo e di 5.000 dollari a settimana in equivalente tempo pieno (FTE) per la manodopera, le strutture e la supervisione di un tecnico, il sistema costa circa 125 dollari per pin di I/O all'ora. Un sistema a 600 pin richiederebbe circa 15 settimane a 75.000 dollari. Questo senza alcuna modifica al progetto. Quindi, in realtà, il costo è probabilmente molto più alto.

Libertà di utilizzare le proprie competenze

NI offre soluzioni per molti tra i più comuni tipi di segnale. Alcune di queste includono segnali digitali ad alta tensione, simulazione di sensori resistivi e schede ARINC 429 e MIL-STD 1553. L'intenzione è che queste schede coprano la maggior parte delle esigenze di I/O. Grazie alla piattaforma aperta e flessibile di NI, è possibile progettare le proprie schede sulla base del kit di sviluppo dei moduli NI SLSC, che fornisce tutti i dettagli necessari per personalizzare circuiti unici compatibili con il resto dell'ecosistema SLSC.

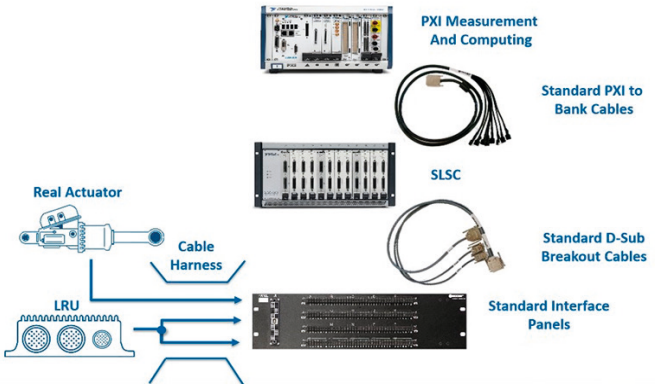


Fig. A - Piattaforme NI SLSC e PXI, i cablaggi e i pannelli di interfaccia standardizzati.

Con questo approccio, è possibile sostituire la progettazione personalizzata con una configurazione che utilizza i componenti di serie. I tester LRU possono essere consegnati pronti per la personalizzazione o possono essere specificamente adattati alle vostre specifiche con un punto di partenza software preconfigurato dai nostri partner.

UNA SOLUZIONE INTEGRATA PER IL MONITORAGGIO DEL TERRITORIO TRAMITE UAS DI SKY EYE SYSTEMS E PLANETEK ITALIA

PLANETEK ITALIA

Sensori avanzati e capacità di analisi per monitorare il territorio e le emergenze ambientali. Planetek Italia e Sky Eye System hanno sviluppato una soluzione integrata per il monitoraggio del territorio con UAS e l'analisi integrata dei dati.

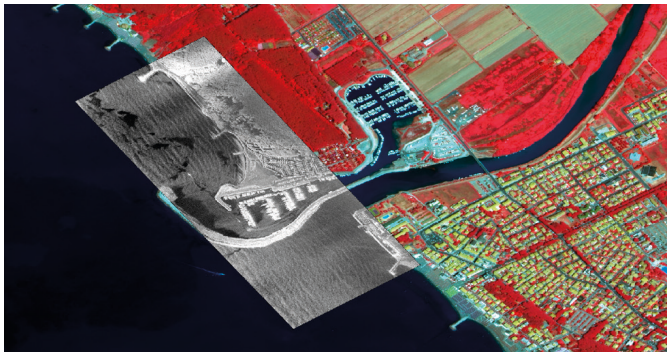
Elaborare i flussi video e i dati ottici e SAR, acquisiti dai sensori a bordo dei droni della famiglia Rapier, tramite algoritmi di intelligenza artificiale al fine di estrarre automaticamente informazioni sensibili e utili agli analisti IMINT e a tutti gli enti che si occupano di controllo del territorio e gestione delle emergenze ambientali: questo è l'oggetto della collaborazione delle due società del settore aerospazio.
Sky Eye Systems ha innovato in modo considerevole il mercato degli UAS di classe mini/light tramite la sua **famiglia di droni, "Rapier":** un sistema UAS (Unmanned Aerial System) ad ala fissa impiegato in missioni di intelligence e di sorveglianza.

Dotato di un'apertura alare di circa 4 metri e un peso inferiore ai 25 kg, il primo modello "Rapier X-25" può essere lanciato da un veicolo militare in movimento (per esempio un blindato Lince) o da un sistema a catapulta pneumatica e sta per ottenere la certificazione militare secondo la normativa STANAG 4703. Rapier X-25 è stato appena acquistato come "cliente di lancio" dall'Aeronautica Militare e consegnato al 32° Stormo di Amendola (Foggia).

La seconda versione è invece il "Rapier X-SkySAR" (peso fino a 30 kg), dotata di sensori elettrottici/infrarossi e dello SkySAR, il più leggero radar ad apertura sintetica del mondo sviluppato dalla stessa Sky Eye Systems.
Una terza versione, attualmente in fase di sviluppo, presenta

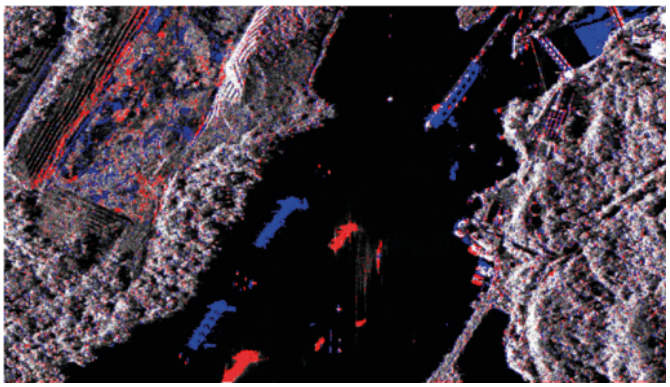
decollo e atterraggio verticali ed è denominata "Rapier X-VTOL". Tra le caratteristiche "Rapier X-VTOL": un peso massimo al decollo di 50 kg (che lo fa rientrare nella Classe Light); un range operativo di 100 chilometri (estensibile ad alcune centinaia di chilometri, grazie al datalink satellitare opzionale); un'autonomia da 5 a 11 ore a seconda della missione; a bordo sensori elettrottici/infrarossi e altri payload opzionali come sensori iperspettrali, Lidar, IFF, SIGINT e anche SAR (Synthetic Aperture Radar), grazie all'estrema flessibilità e modularità della baia payload.

Le tre versioni condividono gran parte delle tecnologie sensibili e fondamentali sviluppate in Sky Eye Systems, quali il layout aerodinamico estremamente ottimizzato, il Flight Control System e la Ground Control Station, sviluppati secondo i massimi standard di sicurezza software-hardware DO178C-DALB, nonché la progettazione strutturale quasi interamente in fibra di carbonio.
Planetek Italia in questa collaborazione ha portato



la trentennale esperienza nella **elaborazione di dati geospaziali per l'IMINT e il GEOINT** al fine di poter estrapolare in modo rapido informazioni utili partendo dai numerosi dati acquisiti a bordo. Tra le principali applicazioni sviluppate e rese disponibili in *real-time* su una postazione *rugged* dedicata all'*exploitation* dei dati, il sistema include *change detection*, data fusion, generazione di modelli 3D e riconoscimento automatico di oggetti.
Le informazioni acquisite dal drone, e i report generati tramite la workstation rugged, possono essere condivisi, in tempo reale, sia con altre unità disposte sul campo che con centri di comando remoti.

Oltre al settore militare, questi UAS hanno anche **numerose applicazioni in ambito civile e governativo**, ad esempio per le attività di security, antincendio e *search & rescue*, ma anche per aerofotogrammetria, monitoraggio di grandi infrastrutture (oleodotti, gasdotti, linee elettriche, reti ferroviarie, autostrade ed altro ancora), per le attività di controllo ambientale e di supporto cartografico nelle emergenze ambientali.
La possibilità di disporre di un drone di questa taglia, non troppo grande da poter essere gestito e lanciato in modo semplice, e di taglia sufficientemente grande per coprire aree molto estese portando a bordo sensori importanti, abbinata ad una postazione *rugged* in grado di elaborare in modo automatico i dati e di estrarre le informazioni utili in *real-time*, rende questa soluzione perfetta nell'ambito delle operazioni di sorveglianza e nelle attività di monitoraggio del territorio in occasioni di emergenze ambientali, occasioni entrambe in cui il fattore tempo è un fattore chiave per la riuscita della missione.



Sky Eye Systems
Sky Eye Systems è un'Azienda aeronautica fondata nel 2017 da un'iniziativa dell'Ing. Massimo Lucchesini, già Amministratore Delegato di Aermacchi e Direttore Operativo di Alenia Aermacchi, e dalla famiglia Tonti della OMA di Foligno (Perugia), che ne detiene la proprietà, con lo scopo di sviluppare una nuova famiglia di "Mini/Light UAS", velivoli a pilotaggio remoto (UAS) del peso compreso tra i 25 e i 50 kg, per impieghi civili e militari di ispezione, mappatura e sorveglianza del territorio.
L'azienda è certificata in accordo agli standard ISO 9001:2015 ed EN 9100:2018, per la progettazione, prototipizzazione, costruzione, addestramento e supporto post-vendita di sistemi a pilotaggio remoto e possiede tutte le risorse e competenze aeronautiche, elettroniche, sistemistiche, per sviluppare in casa le tecnologie abilitanti e sensibili integrate nel Rapier (autopilota/FCS, GCS, aerostrutture).
Per maggiori informazioni: www.skyeyesystems.it
Media Contact: Filippo Carraresi - Tel: +39 050 703706
Email: info@skyeyesystems.it

Planetek Italia
Planetek Italia è una Società Benefit fondata nel 1994 e specializzata in Geomatica, scienze della Terra e soluzioni spaziali. Sviluppiamo sistemi e servizi per l'elaborazione di dati cartografici e satellitari finalizzati alla creazione di conoscenza geo-localizzata. Avendo come valore di riferimento la sostenibilità, operiamo in molti campi di applicazione: monitoraggio ambientale e del territorio, open-government e smart cities, difesa e sicurezza, ingegneria, missioni satellitari scientifiche e di esplorazione dello Spazio. Per maggiori informazioni: https://www.planetek.it/
Media Contact: Antonio Buonavoglia - Tel: +39 0809644200
Email: news @ planetek.it

POLOMARCONI.IT PUNTA SULL'INNOVAZIONE

POLOMARCONI.IT

Polomarconi.it punta sull'innovazione tessendo una rete di collaborazioni strategiche con imprese innovative, università e centri di ricerca per garantire ai propri clienti soluzioni personalizzate allo stato dell'arte, e oltre, per la ricezione, trasmissione e distribuzione del segnale a radio frequenza.
Accompagnare il cliente verso una soluzione sartoriale a lui congeniale è sempre stato il punto di forza di Polomarconi.it. Questa caratteristica di saper collaborare col cliente per giungere alla soluzione ideale è diventata lo spunto di un ambizioso e pluriennale piano di "Open Innovation".
"Open Innovation" è un termine coniato nel 2003 dal Professor Henry Chesbrough oggi Direttore del Garwood Center for Corporate Innovation presso la University of California a Berkeley. Il paradigma dell'innovazione aperta afferma che, per meglio servire i loro mercati, le imprese debbono fare ricorso anche a idee, risorse e competenze tecnologiche che arrivano dall'esterno, per esempio, da altre imprese innovative, da startup, università ed enti di ricerca, fornitori e consulenti. Per fare innovazione aperta bisogna essere disponibili a joint venture e a condividere i risultati con i partner. Avviare e gestire in modo efficace un programma di innovazione aperta è una sfida manageriale complessa che in letteratura va sotto il nome di "Ambidexterity". Significa riuscire a combinare un approccio manageriale volto all'efficienza e alla massimizzazione del margine con uno orientato all'esplorazione, alla ricerca di nuove soluzioni che è un'attività inefficiente per definizione.
L'obiettivo manageriale dell'esplorazione non è il margine, ma la comprensione di un mercato, dei suoi bisogni e la ricerca e creazione del know how necessario a fornirgli soluzioni adeguate.
In Italia sono ormai numerose le imprese che fanno dell'innovazione aperta un pilastro della loro strategia e Polomarconi.it guarda al loro esempio per applicarla con successo. La rete di partner che Polomarconi.it sta costruendo rappresenta nel suo complesso un ampio spettro di competenze, possiede un insieme di risorse importanti e vanta una diffusa presenza su diversi mercati affini tra loro. L'obiettivo primario del piano di innovazione aperta di Polomarconi.it è sempre e comunque la soddisfazione del cliente, dal primo contatto col commerciale fino all'assistenza post-vendita. Integrando il proprio Know How con quello dei propri partner, Polomarconi.it riuscirà a portare ai propri clienti ulteriore valore e soluzioni originali e, qualche volta, anche sorprendenti grazie a idee che provengono da settori diversi. Nel loro insieme, le competenze di Polomarconi.it e dei suoi partner spaziano dai nuovi materiali, ai sistemi MEMS, dai sistemi meccatronici, al controllo ottimo applicato ai sistemi di antenna intelligenti.
Gli obiettivi delle collaborazioni e degli investimenti congiunti sono molteplici: dal fornire prestazioni di picco dei sistemi di comunicazione (che è sempre e comunque il primo obiettivo) alla miniaturizzazione per ridurre gli ingombri dei sistemi a pari prestazioni; dall'aumentare affidabilità e tempo di vita dei prodotti all' automazione, integrabilità e sicurezza dei sistemi.
Un primo importante risultato acquisito da Polomarconi.it è che i suoi prodotti sono compatibili con tutte le radio in commercio e con i principali standard di automazione per semplificare la gestione della sempre crescente complessità della distribuzione e gestione de segnali wireless con la massima sicurezza possibile.

Pur nella contingente e complessa situazione post-pandemica, i risultati delle attività di innovazione sono già evidenti e molto incoraggianti. Polomarconi.it è, infatti, impegnata in collaborazione con imprese eccellenti in progetti ambiziosi ed entusiasmanti, per esempio, nell'ambito delle comunicazioni satellitari ad alta frequenza per sistemi aerei in ambito militare, nello sviluppo di filtri agili o di sistemi di distribuzione e combinazione a radio frequenza automatici e ottimizzati in campo navale, nell'applicazione di sistemi di antenna intelligenti per le comunicazioni ferroviarie e altri ancora.

Ovviamente Polomarconi.it continua sempre a investire per consolidare e crescere le proprie competenze per assicurare ai propri clienti un continuo ed efficace affiancamento e supporto.

PROGRAMMA COPERNICUS E BENEFICI PER IL SETTORE IDRICO
Il ruolo di Serco Italia

SERCO ITALIA

Il programma **Copernicus** dell'Agenzia Spaziale Europea è un insieme di sistemi che raccoglie informazioni da numerose fonti, ossia satelliti di Osservazione della Terra e sensori di terra, di mare ed aviotrasportati. I principali risultati consistono in fornitura di dati satellitari direttamente all'utente finale, oppure la fornitura di modelli e mappe già elaborate, il tutto in maniera **open and free**.

In un periodo di clima estremo come quello che viviamo negli ultimi mesi, l'integrazione di dati di Osservazione della Terra nella modellazione idrologica e nella gestione di bacini può contribuire fortemente alle attività di monitoraggio dei corpi idrici e delle aste fluviali, fornendo una visione **a larga scala** che prenda in considerazione le interazioni esistenti tra un corso d'acqua e il suo bacino idrografico a monte.

I principali benefici diretti e indiretti del programma Copernicus per le attività legate all'idrologia sono: il monitoraggio tramite **interpretazione e confronto dei volumi di invaso dei bacini**, acquisiti dalle immagini satellitari sia ottiche che radar in diversi istanti temporali; il **monitoraggio delle deformazioni, smottamenti e cedimenti** di infrastrutture, quali dighe, canali e opere di manovra, e del territorio tramite analisi interferometriche (radar); la **stima di portata dei principali fiumi** tramite sensori altimetrici satellitari; la analisi e lo studio delle precipitazioni, della loro distribuzione e della loro intensità, con conseguente **modellazione di eventi estremi quali inondazioni e siccità**; la gestione di risorse idriche attraverso l'analisi e la stima dell'umidità sotterranea del terreno;

Nel 2018 la Commissione Europea ha lanciato un'iniziativa per sviluppare i cosiddetti **Data and Information Access Service (DIAS)** per facilitare l'accesso ai dati satellitari e alle informazioni di Copernicus. Fornendo l'accesso ai dati e alle informazioni insieme alle risorse di elaborazione, agli strumenti di analisi e ad altri dati esterni.

ONDA DIAS (www.ONDA-dias.eu) è la piattaforma sviluppata da Serco che, con l'obiettivo di facilitare, favorire ed espandere l'utilizzo dei dati satellitari di Osservazione della Terra e delle informazioni geospaziali, consente agli utenti di costruire e gestire applicazioni in cloud fornendo dati, servizi e supporto.

La piattaforma ONDA DIAS offre **accesso gratuito e aperto** a una vasta gamma di set di dati provenienti da diverse fonti, dalla famiglia Copernicus Sentinels, ad altre missioni satellitari di osservazione della Terra e ai progetti Copernicus Services.

ONDA ospita **uno dei più grandi archivi mai costruiti** per dati e informazioni geospaziali: il servizio offre accesso gratuito e diretto a un repository basato su cloud di oltre **68 milioni di prodotti** (in continuo aumento), che occupano un volume di oltre **42 petabyte di dati memorizzati**.

BREVETTO UNITARIO

Lorenzo Sordini

STUDIO TORTA

La normativa sul brevetto unitario, anche noto in forma abbreviata come UP (Unitary Patent), la cui entrata in vigore è prevista per la fine del 2022 o l'inizio 2023, introduce nel panorama brevettuale dell'Unione europea cambiamenti significativi nella gestione dell'innovazione istituendo un brevetto unico efficace in 25 (nella fase iniziale solo 17) paesi dell'Unione Europea.

SISTEMA ATTUALE

Oggi per tutelare un'invenzione in più paesi europei si possono seguire due vie: la via nazionale al fine di ottenere brevetti nazionali validi sui rispettivi territori o la via del brevetto europeo che, una volta giunto a concessione, viene trasformato in un fascio di brevetti nazionali nei paesi selezionati fra quelli che hanno aderito alla convenzione del brevetto europeo. La situazione attuale prevede quindi che vi siano unicamente brevetti che esplicano la loro efficacia a livello nazionale indipendentemente dall'iter seguito per ottenerli.

IL NUOVO SISTEMA UNITARIO

Il primo punto di rilievo del nuovo sistema è che il brevetto unitario è un diritto sovranazionale indivisibile che produce gli stessi effetti nei 25 paesi (al momento dell'avvio solo 17 paesi) dell'Unione europea. Nelle intenzioni originarie il brevetto unitario avrebbe dovuto coprire l'intero territorio dell'Unione europea e chiamarsi brevetto (com)unitario, ma il veto opposto a questa iniziativa da Polonia e Spagna ha impedito la realizzazione del progetto. Le rimanenti nazioni dell'Unione hanno dato vita alla cosiddetta cooperazione rafforzata per realizzare un titolo unico valido nei territori dei paesi aderenti. La prima condizione necessaria per attuare nel proprio paese il sistema del brevetto unitario è essere membri dell'Unione europea nonché membri della Convenzione del Brevetto Europeo.

Come detto, però, due paesi dell'UE, la Polonia e la Spagna, restano attualmente fuori dal sistema non avendo aderito alla cooperazione rafforzata. Lo stesso vale per la Croazia che è entrata a far parte dell'Unione Europea quando la cooperazione rafforzata era già stata avviata.

L'altra condizione necessaria per rendere il sistema operativo nel proprio paese è quello di ratificare l'accordo denominato "Agreement on a Unified Patent Court" (UPCA), ovvero di adeguare la legge nazionale all'accordo con i necessari passaggi parlamentari. L'accordo comprende materia amministrativa, giurisdizionale e diritto sostanziale in proprietà industriale per cui i paesi membri che ratificano l'accordo devono necessariamente adeguare le proprie leggi nazionali e delegare al nuovo Tribunale UPC l'amministrazione della giustizia per i brevetti europei e i relativi certificati complementari di protezione.

Otto paesi - Cipro, Grecia, Irlanda, Repubblica Ceca, Romania, Slovacchia, Slovenia e Ungheria - non hanno ancora compiuto questo passo.

Oggi il sistema è pronto per entrare in vigore perché è stato raggiunto il numero minimo di paesi previsti dall'accordo e sarà operativo nei seguenti diciassette paesi: Austria, Belgio, Bulgaria, Danimarca, Estonia, Finlandia, Francia, Germania, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Slovenia e Svezia. I paesi che non hanno ancora ratificato potranno aggiungersi in corsa a sistema avviato.

Una volta che una domanda di brevetto europeo giunge a concessione, il titolare può scegliere il brevetto unitario per ottenere un unico titolo brevettuale valido in tutti in 17 paesi sopra identificati oppure un fascio di brevetti nazionali ciascun dei quali esplica la sua funzione sui territori dei paesi selezionati.

Per i paesi aderenti alla convenzione del brevetto europeo diversi da questi 17 paesi vi è la sola opzione di scegliere il brevetto nazionale in accordo con la via già attualmente percorsa. Ad esempio, chi è interessato a tutelare la propria invenzione in Italia, Francia, Svezia, Germania, Svizzera e Regno Unito potrà scegliere di convalidare il brevetto in brevetti nazionali validi in ciascuno di questi paesi o, in alternativa, scegliere il brevetto unitario per coprire Italia, Francia, Svezia e Germania e necessariamente tutti gli altri paesi attualmente all'interno del sistema e convalidare il brevetto europeo in brevetti nazionali nel Regno Unito e in Svizzera. Il brevetto unitario non prevede il meccanismo della convalida nei paesi in cui esplica il suo effetto e, quindi, della traduzione laddove richiesta per i brevetti europei tradizionali secondo il cosiddetto London Agreement. I paesi che hanno aderito accettano dunque che, sul proprio territorio, venga fatto valere un diritto in una lingua diversa dalla propria lingua ufficiale. In caso di controversia il titolare deve fornire se richiesta una traduzione nella lingua del paese se si riscontra una presunta contraffazione o se è instaurato un procedimento di contraffazione.

Inoltre, per un periodo transitorio, se la lingua del procedimento è il francese o il tedesco, il titolare del brevetto europeo con effetto unitario deve fornire una traduzione integrale in inglese del fascicolo del brevetto europeo o se la lingua del procedimento è l'inglese, una traduzione integrale del fascicolo del brevetto europeo in un'altra lingua ufficiale

dell'Unione. Il brevetto unitario, proprio per il suo carattere di titolo indivisibile, deve essere rinnovato per tutti i paesi in cui esplica i suoi effetti. Nonostante ciò, tuttavia, esso può essere concesso in licenza per frazioni di territorio.
La scelta del brevetto unitario determina automaticamente due conseguenze: il mantenimento in solido del brevetto in tutti i paesi aderenti e la scelta della nuova Corte (UPC).

LA RATIFICA NEI VARI PAESI

Un aspetto che conviene prendere in esame è il processo di ratifica perché non tutti i paesi hanno adottato le stesse misure. Se da un lato, quasi tutti i paesi aderenti hanno adottato o stanno adottando una rete di sicurezza nel caso in cui la domanda per brevetto unitario fosse rifiutata, dall'altro lato, vi sono state implementazioni difformi per quanto concerne la sovrapposizione fra brevetto nazionale e brevetto europeo. Sul primo punto, l'Italia ha modificato l'articolo 56 del Codice di Proprietà Industriale e introdotto il comma 4 bis dell'articolo 56 come misura di sicurezza che fa decorrere i tre mesi per il deposito della traduzione della convalida nazionale a partire dalla data del rigetto definitivo della domanda per il brevetto europeo con effetto unitario.
Sul secondo punto, l'Italia ha scelto la via della prevalenza del brevetto europeo sia esso nella forma tradizionale o con effetto unitario. Danimarca, Germania, Estonia, Francia, Ungheria, Austria, Finlandia e Svezia hanno scelto la doppia protezione fra brevetto nazionale e brevetto europeo con effetto unitario. Ciò significa che l'attore potrà decidere se azionare il brevetto nazionale o il brevetto unitario per una contraffazione che ha luogo sul territorio nazionale e quindi di scegliere il Tribunale nazionale o l'UPC.
Danimarca, Ungheria, Polonia, Slovenia, Finlandia e Svezia hanno optato per la doppia protezione con brevetto nazionale e brevetto europeo tradizionale senza particolari condizioni a parte la Slovenia.
In questo capitolo è ancora opportuno illustrare l'estensione territoriale del brevetto europeo con effetto unitario per Danimarca, Francia e Paesi Bassi che presentano alcune particolarità. L'adesione della Danimarca alla Convenzione sul brevetto europeo non comprende le Isole Fær Øer e la Groenlandia sebbene facciano parte del Regno di Danimarca per cui il solo brevetto nazionale danese è efficace anche su quei territori, mentre il brevetto europeo convalidato in Danimarca è efficace solamente nella penisola della Danimarca.
La Francia ha deciso che un brevetto europeo tradizionale e un brevetto europeo con effetto unitario avranno efficacia in Martinica, Réunion, Mayotte, Saint Barthélemy, Saint-Pierre e Miquelon, Saint-Martin e le Terre australi e antartiche francesi, nonché a Wallis e Futuna.
La decisione della Francia si applica solo in parte alla Nuova Caledonia e alla Polinesia francese. Questi Paesi hanno competenze proprie in materia di proprietà industriale e lo Stato francese non ha l'autorità di legiferare in materia. Comunque la Nuova Caledonia e la Polinesia francese eserciteranno presto le loro competenze in materia e dovranno scegliere se aderire al brevetto unitario o meno.
Il regno dei Paesi Bassi, per quanto ci è dato di comprendere, ha optato per la protezione nei cosiddetti territori d'oltremare ad eccezione di Aruba che ha una propria legge brevetti. Per cui un brevetto nazionale olandese, la convalida nel Regno dei Paesi Bassi di un brevetto europeo tradizionale ed un brevetto europeo con effetto unitario hanno efficacia sul territorio europeo di questo paese ma anche nelle isole caraibiche di Curaçao, Sint Maarten, Bonaire, Sint Eustatius e Saba.

IOTA, RETE DECENTRALIZZATA PER APPLICAZIONI MISSION CRITICAL

La DLT efficiente, economica, scalabile, sostenibile

TELECONSYS

Le blockchain sono utilizzate in molti settori industriali. Ma quale sono i vantaggi delle blockchain? In estrema sintesi tra i principali vantaggi c'è la capacità di impedire modifica e cancellazione di informazioni da un registro. Una sorta di database inviolabile. Tuttavia le blockchain hanno anche gravi limitazioni. In primo luogo la sicurezza del registro deriva dalla collaborazione di molti attori che agiscono per interesse economico. Ciò limita le prestazioni ottenibili perché si crea un conflitto di interessi tra chi le usa e chi le gestisce. Questo è uno dei motivi che hanno portato all'idea di creare blockchain private che tuttavia non sono in grado di produrre lo stesso livello di sicurezza, riproducendo in modo inefficiente esattamente le caratteristiche funzionali di un database non relazionale. Esiste un'alternativa? Si, la rete IOTA.

IOTA è un progetto derivato dalla blockchain che ne conserva gran parte dei principi funzionali ma ne supera i limiti. In primo luogo non vi è alcuna distinzione tra utenti e gestori della rete: ogni nodo diviene un validatore di transazioni precedenti quando ne immette una nuova. In IOTA il modello organizzativo della rete non è competitivo ma collaborativo. Ciò elimina il mining, il suo costo energetico e ogni limitazione prestazionale derivata. In IOTA non occorre pagare fee per immettere dati nel registro e ciò, unito al basso costo operativo dei nodi che non eseguono il mining, elimina anche la variabilità del costo del servizio subito dai client delle blockchain. Infine in IOTA il registro non è organizzato in blocchi. Le transazioni sono direttamente collegate a precedenti. Questo accorgimento permette ai nodi di immettere nuove transazioni senza essere sincronizzati con tutti gli altri nodi della rete nella prodizione di del prossimo blocco. Questa flessibilità, oltre a ridurre ulteriormente le caratteristiche minime richieste a un nodo, permette alla rete di operare in modo asincrono eliminando ogni "collo di bottiglia". IOTA fornisce di fatto il compromesso ideale tra una rete privata e una pubblica garantendo costi e prestazioni di una rete privata e sicurezza e decentralizzazione di una rete pubblica.

Ci sono poi molti aspetti pratici derivati che possono divenire molto utili per la realizzazione di applicazioni critiche. Per esempio l'assenza di fee permette di inserire nel registro transazioni che non spostano token ma contengono semplicemente dati (fino a 32 KB). Un altro aspetto pratico consiste nell'ottenere la gestione immediata delle transazioni. Nelle blockchain infatti l'inserimento nel registro di una transazione è rallentato da molteplici fattori. In IOTA invece, i client di un nodo possono ricevere una transazione appena il nodo ha completato la validazione di almeno due transazioni precedenti, operazione che dura tipicamente pochi secondi. IOTA poi non è solo un registro distribuito. Grazie alle sue caratteristiche funzionali è la piattaforma ideale su cui costruire applicazioni decentralizzate come ad esempio un sistema di comunicazione sicuro, non censurabile, non intercettabile e riservato. In questo esempio due client possono usare IOTA per scambiarsi messaggi criptati. Devono solo condividere l'indirizzo iniziale della sequenza. IOTA è utilizzato come sistema di trasporto sicuro dove i client possono usare qualsiasi nodo della rete per inviare e ricevere messaggi e nonostante la rete sia pubblica saranno gli unici a poterli decifrare. La persistenza dei messaggi nel registro garantisce la ricezione anche in differita e dato che nel registro non sono memorizzate informazioni relative ai client che hanno generato i messaggi, i mittenti non sono neppure georeferenziati.

Ovviamente è anche possibile attivare una propria rete IOTA dedicata. L'unica accortezza richiesta è che sia comunque composta da nodi gestiti da operatori indipendenti al fine di garantire l'assenza di un "single point of control" che renderebbe possibile bloccare l'intera rete. La rimozione del single point of control è il vero punto di forza delle blockchain e il principale motivo per chi dovrebbero essere prese in considerazione da chi progetta applicazioni mission critical. La presenza di personale con indispensabili credenziali amministrative è uno dei fattori su cui si basano attacchi informativi. L'eliminazione di questo fattore di rischio in un sistema centralizzato è sostanzialmente impossibile. Al contrario, una applicazione progettata sul modello decentralizzato che sfrutta una rete decentralizzata come contenitore sicuro, diviene virtualmente inattaccabile.

SINERGIE TRA SISTEMI OT SATELLITARI AD ALTE PRESTAZIONI E COSTELLAZIONI DI MICRO E PICCOLI SATELLITI

Space Economy: trasformazione del settore spaziale

Autori: L. Soli, V. Mastroddi, A. Nassisi, C. Ciancarelli, A. Intelisano

THALES ALENIA SPACE

La Space Economy è un ecosistema complesso, che integra industrie manifatturiere ad alto contenuto tecnologico e servizi avanzati con una commistione tra diversi soggetti favorendo trasferimenti di conoscenze ed uno sviluppo sinergico ad alto tasso di innovazione. Le costellazioni di piccoli satelliti OT (Osservazione della Terra) stanno guidando le richieste del mercato verso informazioni di OT più vicine alle esigenze dell'utente finale, sostituendo immagini e servizi tradizionali. Una architettura guidata dalla complementarità tra satelliti OT ad altissime prestazioni (VHP) e costellazioni Small/Micro-SAT permette di migliorare le prestazioni temporali come reattività, rivisitazione ed età dei dati con costi contenuti ed un rapido dispiegamento della costellazione. La tecnologia SAR, grazie alla capacità di rilevamento giorno e notte ed in ogni condizione atmosferica, è particolarmente votata a garantire l'osservazione in condizioni di emergenza e sicurezza. Un campionamento continuo della superficie del pianeta su base ripetitiva e regolare è un importante fattore abilitante per la valutazione dei cambiamenti sull'area di interesse con osservazioni sistematiche. Le orbite sincrone solari (SSO) sono in grado di fornire una copertura globale a tutte le latitudini con la sola limitazione di osservare la stessa area sempre alla stessa ora locale, il che potrebbe essere prezioso per alcune applicazioni specifiche; nel contempo le orbite con un angolo di inclinazione inferiore (non orbite polari o SSO), possono osservare la stessa area con tempi locali e angoli di aspetto diversi (solitamente molto più grandi dell'SSO). La costellazione di satelliti radar italiani COSMO Sky-Med, offre già un contributo significativo alla gestione delle emergenze, fornendo immagini SAR tempestive ed accurate come ad esempio dalla mappatura delle inondazioni alla valutazione dei danni dei terremoti durante un numero considerevolmente elevato di eventi di emergenza reale e fornisce una copertura interferometrica completa @ 3m di risoluzione in banda X del territorio italiano ogni circa due settimane ("Programma Map-Italy"). La reattività del sistema CSK in modalità di emergenza è di 18 ore e con il dispiegamento di una piccola costellazione di satelliti SAR, composta ad esempio da 6 satelliti, consentirebbe sia il miglioramento della risoluzione temporale sia di avere la possibilità di diverse configurazioni di costellazione per l'interferometria e la copertura sistematica. Il satellite SAR è in grado di accedere sul lato destro e sinistro w.r.t. la direzione di volo.

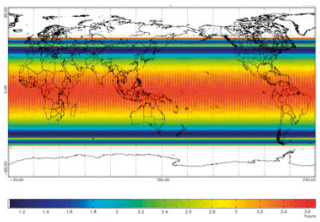


Fig. 1

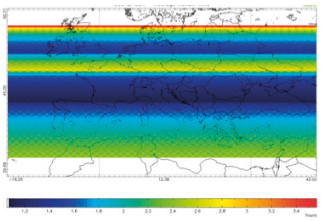


Fig. 2

Considerando un range di accesso in termini di angolo di incidenza di 20°-60°, la configurazione (Fig. 1) con 6 satelliti disposti su tre piani orbitali in orbita inclinata consente un tempo medio di rivisitazione inferiore a 3,6 ore sull'area accessibile (che per l'orbita di scelta è di circa ±60°) con un tempo medio di rivisita inferiore a 2,5 ore (Fig 2) sull'area Europa e Mediterraneo (che in questo caso rappresenta le Aree di Interesse). Quindi un mix di diverse costellazioni potrebbe essere indirizzato per trarre il massimo vantaggio dal design di entrambe le costellazioni ed i possibili principali vantaggi sono: accessibilità globale grazie alle orbite polari, il più alto tempo di rivisitazione sull'area di interesse grazie all'orbita inclinata più l'addizionale capacità di accesso fornita dalla configurazione SSO, monitoraggio sistematico e costante dell'area di interesse, acquisizione su richiesta, qualità dell'immagine molto elevata. Come mostrato nelle seguenti mappe colorimetriche (Fig 3 e 4) l'unione delle due costellazioni consente di ottenere un tempo medio di rivisitazione sull'Area di Interesse di ~ 1,5 ore beneficiando così di entrambi gli asset nazionali e sfruttando al meglio l'investimento nazionale. Un maggiore numero di satelliti potrà ulteriormente incrementare sia le prestazioni di rivisita che le capacità di coverage della costellazione. Thales Alenia Space Italia, in qualità di System Engineer di COSMO Sky-Med, ha una posizione unica per definire al meglio la piccola costellazione di Satelliti SAR in modo complementare offrendo all'utente finale il miglior utilizzo di High Performance Satellite insieme ad un'elevata risoluzione temporale rigorosamente necessario per alcune applicazioni critiche.

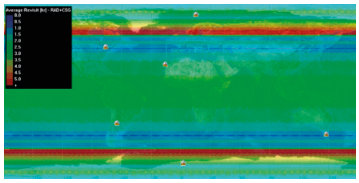


Fig. 3

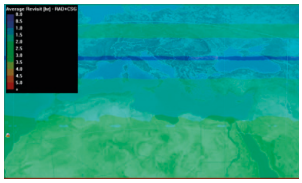


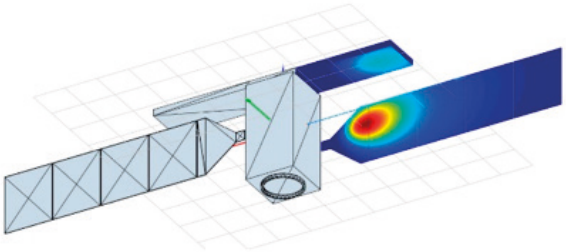
Fig. 4

SATELLITE PLUME IMPINGEMENT

Effetto del getto prodotto da propulsori spaziali

Autori: A. Adriani, A. Binci, A. Marchetti, A. Montani

THALES ALENIA SPACE



Tutti i veicoli spaziali sono generalmente dotati di sistemi di propulsione, chimici o elettrici, in grado di effettuare manovre di controllo dell'orbita e di assetto che vengono eseguite da propulsori il cui getto di scarico può interagire con le superfici del veicolo. È il fenomeno del *plume impingement* che sin dalle prime fasi di progettazione di qualsiasi missione spaziale viene valutato con attenzione per garantire le prestazioni richieste. Nel vuoto spaziale il getto si propaga diffondendosi non solo lungo l'asse del propulsore ma anche lateralmente e "all'indietro" (Back Flow) e di conseguenza, in base anche all'alloggio dei propulsori sul veicolo, può interessare differenti parti del satellite e relative appendici (pannelli solari, antenne, ecc).

Nel caso di **propulsori chimici** (liquido mono- propellente o bi-propellente) i prodotti di combustione espulsi subiscono una forte espansione nella quale il gas attraversa diversi regimi, caratterizzati da un diverso livello di rarefazione del flusso. In tale direzione, la caratterizzazione del regime avviene per mezzo di un parametro adimensionale chiamato numero di Knudsen (Kn), definito come il rapporto del cammino libero medio molecolare e una dimensione caratteristica (L). Per l'analisi del flusso continuo vengono solitamente utilizzati codici di fluidodinamica computazionale (CFD) che implementano le equazioni di Navier-Stokes. I flussi molecolari e transitori liberi, dove non si può più considerare il gas come un continuo, sono governati dall'equazione di Boltzmann. In questi casi si utilizza un approccio probabilistico, noto come metodo Direct Simulation Monte Carlo (DSMC).

Nei **propulsori elettrici** (ad effetto Hall ed a Ioni), che sono in grado di offrire impulsi specifici molto più elevati rispetto ai tradizionali propulsori il getto emesso dal motore è formata principamente da ioni (particelle cariche). In tali propulsori, il propellente neutro (tipicamnete Xeno) è prima ionizzato e poi accelerato ed espulso. Nello specifico, le particelle ionizzate positivamente vengono accelerate attraverso la parte definita "anodo" mentre quelle negative sono emesse da un catodo, impiegato in combinazione per neutralizzare il più possibile il plasma espulso. Di conseguenza, la plume per questo tipo di motori è costituita da diversi elementi: principalmente ioni positivi a diversi livelli di energia e ionizzazione, elettroni, propellente neutro e materiali erosi dal corpo dello stesso propulsore. L'espansione del getto per questo tipo di motori è regolata da diversi fattori tra cui l'energia cinetica ionica, la pressione plasmatica interna, le collisioni tra particelle per cui si definiscono due regioni principali di regime: una prossima al propulsore (Near Field, circa 1-2 raggi del propulsore) dove il numero di collisioni è elevato e dove si risente della presenza del propulsore in termini di campo elettrico/magnetico. Per l'analisi di quetsa zona, tecniche come la simulazione diretta (DSMC) o Particle-in-cell (PIC) sono preferite e largamente utilizzate mentre nella regione "lontana" (Far Field) dal propulsore, dove le collisioni risultano praticamente assenti, anche l'uso di modelli basati su metodi semi-analitici fornisce risultati accurati.

In generale, per entrambe le tipologie di propulsione, gli effetti del *plume impingement* sulle superfici investite si caratterizzano in termini di forze e momenti dinamici con conseguente disturbo dell'assetto del satellite e del suo puntamento nominale, in termini di flussi termici, contaminazione e fenomeni erosivi di sputtering che possono indurre variazioni delle proprietà termomeccaniche ed ottiche degli apparati coinvolti. In aggiunta è da ricordare nel caso di motori elettrici, l' accumulo di cariche elettriche che possono generare dannose scariche elettrostatiche e fenomeni di compatibilità EMC.

In **Thales Alenia Space Italia** sono stati sviluppati specifici tool per l'analisi di sistema per entrambe le tipologie di propulsione (PITOT per la chimica e PITEL per la elettrica). I software hanno una architettura modulare, intuitiva e duttile oltre che la capacità di gestione del fenomeno del *plume impingement* direttamente sulle superfici satellitari tramite le routine di importazione e management del CAD. L'implementazione di modelli analitici e semianalitici dell' espansione della plume e dei fenomeni di interazione con le superfici satellitari consentono di eseguire rapidamente, fin dalle prime fasi di un progetto, analisi e valutazioni accurate con costi computazionali estremamente bassi.

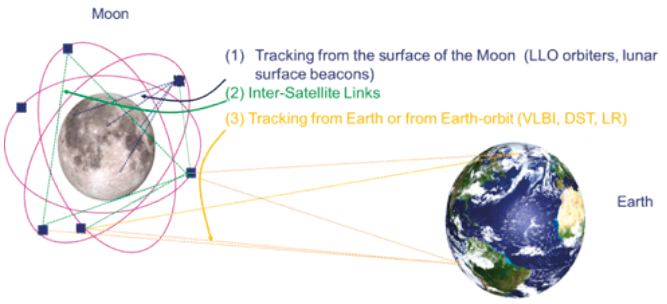
STUDIO DI FATTIBILITÀ PER UN SISTEMA DI NAVIGAZIONE SATELLITARE LUNARE

Autori: C. Stallo, E.E. Zini

THALES ALENIA SPACE

Negli ultimi anni, a livello internazionale, si è di nuovo risvegliato l'interesse per l'esplorazione umana della Luna, grazie anche alle recenti scoperte di acqua al Polo Sud. Nell'ultimo decennio sono state pianificate numerose missioni da parte delle maggiori agenzie spaziali mondiali, in collaborazione con l'industria, per consentire un accesso stabile alla Luna tramite la realizzazione di infrastrutture permanenti in ambiente cis-lunare e su suolo lunare. In tutte le iniziative proposte, le comunicazioni e la navigazione satellitari giocheranno un ruolo fondamentale per garantire una elevata continuità di operazioni nel volume di servizio lunare. Il programma Artemis di NASA, che ha come obiettivo quello di riportare l'uomo sulla Luna nei prossimi anni, rappresenta un grande volano per la definizione di servizi per lo sfruttamento commerciale della Luna, creando un modello di riferimento da estendere poi ad altri pianeti più lontani dalla Terra, come Marte.

In questo contesto, Telespazio e Thales Alenia Space stanno conducendo due studi di fattibilità nell'ambito dell'iniziativa Moonlight lanciata dall'Agenzia Spaziale Europea: il primo per la definizione di un sistema di comunicazione e navigazione lunare e dei servizi associati (Lunar Communication and Navigation Services (LCNS)), il secondo sull'identificazione e progettazione dei concetti chiave per la progettazione di un sistema di radionavigazione lunare (Lunar Radio Navigation System (LRNS)), quali gli algoritmi e le tecnologie per la determinazione orbitale e sincronizzazione dell' orologio a bordo (ODTS) del satellite, tecniche di modulazione del segnale per il servizio di navigazione one-way e i sistemi di riferimento selenodetici e di tempo. Come per il GNSS terrestre, lo scopo principale dell'ODTS è quello di fornire regolarmente dati accurati sulle effemeridi e sulle correzioni per l'orologio di bordo dei satelliti nel messaggio di navigazione ad un utente LCNS al fine di consentire la stima della propria posizione ad una data epoca. Lo stato dell'arte dell'OD per missioni lunari/interplanetarie consiste principalmente in tecniche di tracking two-way dalla Terra. Esso è realizzato tramite il link TT&C (Telemetry, Tracking and Command) tra i satelliti e le stazioni a terra opportunamente distribuite. Sebbene questo metodo sia stato usato con successo in tutte le missioni lunari, i requisiti sulle prestazioni per LRNS sono stringenti, portando ad analizzare altre opzioni sia tradizionali che innovative:



Tecniche ODTS per LRNS

- Tecniche differenziali, come Very-Long-Baseline Interferometry (VLBI) e Same Beam Interferometry (SBI), nonché laser ranging (LR), sono tecniche di tracking da Terra che offrono vantaggi in termini di bassi livelli di rumore nelle misure ottenute, ma che apportano un'alta complessità rispetto alla soluzione classica di tracking tramite TT&C.
- Un notevole miglioramento delle prestazioni si potrebbe ottenere tramite l'utilizzo di misure collezionate direttamente in ambiente lunare grazie all'uso di inter-satellite links (ISL) tra i satelliti LCNS o a misure di ranging da ricevitori in orbita o su suolo lunare. In questo caso, il miglioramento delle prestazioni si deve alla migliore distribuzione spaziale delle osservazioni processate.

La funzione di sincronizzazione del tempo del sistema ODTS è preposta a correggere la deriva dell'orologio a bordo di uno specifico satellite. Tra le diverse soluzioni possibili, i RAFS (Rubidium Atomic Frequency Standard) sono identificati come la miglior soluzione in termini di prestazioni ottenibili e complessità. Il processo di sincronizzazione prevede 3 fasi:

- Osservazione dell'offset/drift dell'orologio rispetto al tempo di riferimento del sistema;
- Generazione delle correzioni in base al modello scelto per definire l'evoluzione dell'orologio di bordo;
- Trasmissione delle correzioni tramite time-transfer a due vie con Deep Space Transponder (DST).

L'altro nodo chiave nella progettazione di LRNS è la definizione dei segnali di navigazione. Lo schema di accesso multiplo al canale proposto è il CDMA (Code Division Multiple Access); grazie all'uso dei codici Pseudo Random Noise, i segnali CDMA sono ottimizzati per massimizzare l'accuratezza della stima del tempo di arrivo del segnale da parte di un ricevitore LCNS. Per quanto riguarda la modulazione, BPSK (1) sulla componente dati e BOC (5,1) su quella pilota del segnale LRNS sono state identificate come le soluzioni candidate per alta robustezza, ottime prestazioni e ridotta complessità.

RADAR METEOROLOGICI VAISALA A DOPPIA POLARIZZAZIONE: PRESTAZIONI ANCORA PIÙ POTENTI CON I TRASMETTITORI A STATO SOLIDO

L'innovazione nel radar meteorologico

VAISALA

Con il radar meteorologico **WRS400** (in banda **X**) e il **WRS300** (in banda **C**) VAISALA ha introdotto in uso operativo l'impiego di trasmettitori con amplificatori di potenza allo stato solido (Solid State Power Amplifier – SSPA). I trasmettitori a stato solido hanno il pregio di lavorare a basse tensioni e nel caso di rottura di un amplificatore l'unica conseguenza sarebbe la diminuzione della potenza trasmessa e non il completo spegnimento, come nel caso di trasmettitori di tipo magnetron. I trasmettitori a stato solido forniscono una maggiore precisione nell'osservazione, nella sensibilità e nella qualità del tracciamento. Inoltre le prestazioni wide-band eliminano virtualmente il rischio di interferenze.

Il radar meteorologico Vaisala, con trasmettitore a stato solido, presenta un design compatto, dove il trasmettitore e il ricevitore sono collocati sul retro dell'antenna (soluzione AMR - Antenna Mounted Receiver); questa soluzione consente una struttura estremamente corta di guida d'onda corta ed il percorso del segnale breve e semplificato riduce al minimo l'attenuazione del segnale e fornendo una migliore sensibilità. L'antenna è un altro elemento importante della soluzione Vaisala per il radar meteorologico in doppia polarizzazione. L'antenna è espressamente ottimizzata per misure affidabili e di qualità. Ogni antenna prodotta da Vaisala viene misurata e i test report forniti al cliente in fase di collaudo tecnico. Il disegno innovativo del piedistallo consente che l'antenna e il sistema ricetrasmittente possono essere fissati vicino al centro di gravità, senza necessità di impiego di pesanti contrappesi. Il piedistallo combina una struttura leggera con un basso momento d'inerzia e un meccanismo di trasmissione a doppia cinghia, scelta questa molto affidabile in quanto non vi è gioco nel sistema di distribuzione (ciò invece è tipico dei sistemi con meccanismo a ingranaggio). Questa soluzione è ispirata a principi di bassa manutenzione e non c'è necessità di sostituire olii o lubrificare il piedistallo.

Le altre principali caratteristiche del radar meteorologico Vaisala, che aumentano l'affidabilità dell'intero sistema sono:

- il disegno di protezione contro i fulmini: le scariche atmosferiche e i relativi sbalzi di tensione sono fra le primarie cause di interruzioni di operatività dei radar. La protezione contro i fulmini è integrata nel disegno del radar meteorologico Vaisala (trasmettitore/antenna/piedistallo);
- il BITE "Built-in Test Equipment" (BITE) che è di ausilio per una facile ricerca guasti ed, in alcuni casi, consente di ricevere un avvertimento in anticipo sulla degradazione di funzionamento prima che si verifichi il guasto effettivo;
- il logging esteso dei messaggi;
- la capacità di assistenza tecnica da remoto.

Una corretta elaborazione del segnale è fondamentale per massimizzare i vantaggi di un radar meteorologico con trasmettitore a stato solido. Gli amplificatori a stato solido utilizzano una potenza di picco molto inferiore rispetto alla tecnologia tipo magnetron, migliorando l'affidabilità dell'intero sistema, pur garantendo un'eccellente risoluzione e la completa copertura delle misure senza gap di dati.

Dotato di algoritmi proprietari all'avanguardia, inclusa la classificazione delle idrometeore HydroClass™, il radar meteorologico Vaisala utilizza misurazioni delle polarizzazioni in un collaudato algoritmo di logica fuzzy per classificare i bersagli in categorie come grandine, graupel, pioggia, neve e neve bagnata, nonché bersagli non meteorologici, con i vantaggi di una migliore qualità dei dati per poter rilasciare avvisi più accurati in caso di condizioni meteorologiche avverse.

I costi del ciclo di vita dei trasmettitori a stato solido sono bassi perché non richiedono la sostituzione di parti consumabili costose, quali ad esempio il magnetron. La manutenzione è un fattore importante nel radar meteorologico, e gli amplificatori di potenza allo stato solido sono progettati per durare per l'intero ciclo di vita del sistema. La durata operativa di un trasmettitore a stato solido è stimata pari a 20 anni.

COME BEDROCK STREAMING È MIGRATO DA VMWARE A VATES

Una delle tante storie di successo dei clienti Vates

di Marc Pezin & Charles-H. Schulz

VATES

Le cose stanno cambiando nel campo della virtualizzazione. Nel 2021, l'azienda ha scelto di migrare la propria infrastruttura on-premise da VMware a XCP-ng. Una volta completata la migrazione, Bedrock ha accettato di rispondere ad alcune nostre domande.

Chi è Vates?

Vates è un fornitore di software con sede a Grenoble che sviluppa soluzioni Open Source sicure e chiavi in mano per la gestione dell'infrastruttura ICT e la virtualizzazione. In particolare, sviluppa il prodotto **Xen Orchestra**, la sua soluzione di backup e gestione dell'infrastruttura ICT e **XCP-ng**, il suo hypervisor basato su **Xen**.

Nell'ambito della dinamica di crescita internazionale sarà Leandro Aglieri a guidare lo startup e lo sviluppo della filiale italiana di VATES, che annovera già tra i suoi clienti realtà importanti come Generali Operation Services Platform, Starhotels, Ever (Gruppo Esseco) e Camozzi Group.

"Ho lavorato con VATES per più di un anno in Italia – dichiara Leandro Aglieri – *e abbiamo compreso le enormi potenzialità della società e delle tecnologie open source di virtualizzazione che propone. Sono certo potrà essere attore strategico nel mondo della Difesa e della Cybersecurity in Italia".*

Chi è Bedrock Streaming?

Bedrock Streaming è una società francese che sviluppa una piattaforma di video streaming. Questa piattaforma è venduta in white label ad altri clienti, principalmente emittenti europee. In Francia, la piattaforma è utilizzata da 6play (M6) e Salto.

Bedrock ha più di 45 milioni di utenti in 5 paesi diversi e più di 12 anni di esperienza nel campo. Vincent Gallissot - Lead Cloud Architect @Bedrock, Senior Site Reliability Engineer - spiega perché parte della loro infrastruttura è nel cloud mentre altri server rimangono in sede.

"L'elasticità del cloud soddisfa le nostre esigenze aziendali, il che ci consente di adattare i nostri costi all'utilizzo effettivo. Per altre esigenze, come strumenti interni (Git, metriche, log), la nostra CDN, apparecchiature video o gateway dedicati con ISP francesi, continuiamo a utilizzare i nostri datacenter di Parigi. Riduciamo i costi gestendo noi stessi alcuni servizi che non necessitano della scalabilità del cloud. D'altra parte, per strumenti critici (come il nostro Git), essere nel cloud ci bloccherebbe troppo ed è importante per noi non mettere tutte le uova nello stesso paniere."

VATES Italy Board (Charles Schulz – CSO, Nithida Vialle – CFO, Olivier Lambert – CEO, Leandro Aglieri – CEO Vates Italy)

Prima del 2021 e della loro transizione alla nostra soluzione di virtualizzazione XCP-ng, l'intera infrastruttura Bedrock, sia nel cloud che nei loro data center, era gestita con VMware, una situazione che non si adattava a Vincent.

"Siamo un piccolo cliente (non abbiamo 5.000 hypervisor) e i nostri ticket di supporto o richieste di funzionalità non sono stati ricevuti con la serietà che ci aspettavamo. Inoltre, avevamo vSphere 6.x e dovevamo migrare a 7.x, che era un grande progetto su cui dovevamo investire molto tempo. Nella fase precedente al trasferimento del nostro datacenter, abbiamo colto l'occasione per cambiare la nostra soluzione di hypervisor e scegliere un player francese disposto a supportarci. Amiamo la mentalità e la serietà del team Vates, la scelta dell'Open Source e la grande trasparenza delle decisioni."

La loro infrastruttura in loco è destinata agli ambienti di produzione utilizzati dai clienti che utilizzano le loro piattaforme o dai team interni. Per Bedrock Streaming, la cosa più importante è la stabilità della piattaforma.

"Da qualche anno seguiamo l'evoluzione di Vates, così come il progetto Xen Orchestra. Non abbiamo testato altri 200 prodotti, abbiamo provato XCP-NG + Xen Orchestra e l'abbiamo adottato! L'idea era di utilizzare tools che consumano molte risorse (Virtual Machine di grandi dimensioni), ma anche con prestazioni molto buone (come i nostri Network Load Balancer) e con un'esperienza utente UX intuitiva (lavoriamo principalmente sul cloud, l'obiettivo è non spendere 2 ore per poter spostare una VM). Il resto delle funzionalità era piuttosto standard nell'azienda: autenticazione SAML, backup incrementali, alta disponibilità delle VM (failover automatico a caldo), tagging delle VLAN, supporto NFS, ecc."

A Vincent è stato chiesto quali fossero i principali vantaggi di XCP-ng per loro:

“Fa quello che vogliamo, che è già un grande vantaggio!”

È efficiente, ne abbiamo visibilità (a causa dell’aspetto Open Source, non è una scatola nera), è affidabile e le nostre domande hanno una risposta rapida. Le nostre richieste di funzionalità vengono prese sul serio così come le nostre segnalazioni di bug e la frequenza di rilascio è sorprendente. Infine, gli aggiornamenti sono semplici: non c’è bisogno di fare 200 domande prima di installarli.”

Abbiamo chiesto a Vincent come si sentiva riguardo alla nostra assistenza durante la migrazione:
“Ottima, abbiamo spiegato il nostro contesto, che stavamo per installare i nostri hypervisor uno dopo l’altro piuttosto che acquistare un’intera batteria di server nuovi: era quindi necessario fare un doppio giro e andare abbastanza velocemente. Il team di Vates ha subito colpito nel segno offrendoci uno script e strumenti per aiutarci con la migrazione. Abbiamo reinstallato il nostro primo hypervisor sotto XCP-NG, abbiamo configurato Xen Orchestra come volevamo e meno di un mese dopo la migrazione della prima VM, l’intero parco è stato migrato, tutti gli hypervisor giravano sotto XCP-NG, tutto questo è andato in produzione senza tempi di inattività.”

“Grazie allo script di importazione delle VM in formato ovf lo abbiamo utilizzato per creare un altro script che esportasse la VM sul lato VMware, mappasse le interfacce di rete e disco e infine importasse la VM. Quindi il processo di migrazione è stato completamente automatizzato. Le piccole VM sono state migrate e rimesse in produzione in pochi minuti.”

“La gestione e la configurazione per la produzione di XO/XCP-NG è stata eseguita da due persone ed è durata alcuni giorni, compresi i test di importazione VM. Aggiungiamo 1 mese in più a 6 per migrare poco più di 200 VM.”

Alla Vates, siamo molto felici di esserci uniti a Bedrock nell’avventura di Xen e di essere stati scelti per sostituire VMWare.
Questa migrazione dei sistemi di produzione del nostro Cliente senza tempi di fermo è per noi un’opportunità per dimostrare che è molto semplice migrare da altre soluzioni di virtualizzazione.

LA LEGGE SUL CYBER REPORTING AIUTA A COMBATTERE IL RANSOMWARE, MA IL RECUPERO DEI DATI È ESSENZIALE

Rick Vanover, Sr Director Product Strategy

VEEAM

Con la firma da parte del presidente Biden su una legge sugli stanziamenti omnibus da 1,5 trilioni di dollari, il governo federale degli Stati Uniti è pronto a spendere miliardi di dollari per rafforzare la cybersicurezza e l'informatica all'interno delle sue agenzie. Ma il pacchetto di spesa affronta inoltre una delle sfide più persistenti per identificare e mitigare i cyberattacchi ad ampio raggio nell'infrastruttura della nazione, compreso il ransomware: condivisione dei dati e notifica di una violazione informatica. Questa legge aiuterà a fornire un'intelligence azionabile sulle minacce, per aiutare a prevenire l'emergere di ransomware e altre minacce. Essa mostra anche la necessità di incorporare strumenti di gestione e recupero dei dati negli ambienti IT, sia per salvaguardare le informazioni che per preservarle in caso di attacco.

Il ruolo del reporting nel mitigare il ransomware

Ci si aspetta che i requisiti di segnalazione del Cyber Incident Reporting for Critical Infrastructure Act entrino pienamente in vigore una volta che la CISA determina come definire le entità coperte dalla legge, ma è probabile che le politiche precedenti limitino l'applicazione alle industrie di infrastrutture critiche.

Le entità saranno tenute dalla legge a segnalare un incidente informatico coperto non più di 72 ore dopo che uno "crede ragionevolmente" di essere stato attaccato. Dovranno segnalare qualsiasi pagamento di ransomware effettuato entro 24 ore. Queste entità dovranno fornire alla CISA informazioni sui sistemi informativi, le reti o i dispositivi colpiti, così come "le vulnerabilità sfruttate e le difese di sicurezza che erano in atto, così come le tattiche, le tecniche e le procedure pertinenti a tale incidente", e quali informazioni si ritiene siano state accessibili da individui non autorizzati. Le misure permetteranno alle entità di ricevere precocemente informazioni critiche sulle minacce, permettendo loro di rafforzare e applicare patch ai sistemi software per aiutare a prevenire la diffusione di un attacco.

In un momento in cui gli ambienti IT stanno diventando più complessi, con entità che perseguono un mix di multi-cloud, cloud ibrido e tecnologia on-prem, le soluzioni di gestione e protezione dei dati sono diventate più essenziali.

Salvaguardare i vostri dati dalle minacce informatiche

Secondo il Veeam® Data Protection Trends Report 2022, su più di 3.000 responsabili IT globali, l'89% riferisce un divario tra la quantità di dati che possono permettersi di perdere in caso di interruzione e la frequenza con cui viene eseguito il backup dei dati.

Un altro 18% degli intervistati riferisce che i loro dati non sono sottoposti a backup. Con gli attacchi ransomware in aumento, assicurarsi che i dati non siano solo sottoposti a backup, ma completamente recuperabili è diventato più critico che mai. Mentre il Cyber Incident Reporting for Critical Infrastructure Act fornirà ai leader tecnologici informazioni preziose sugli obiettivi degli aggressori, le entità avranno ancora bisogno di avere salvaguardie in atto per garantire che i loro dati siano protetti e recuperabili in caso di una violazione informatica.

Per coloro che sono stati violati in un attacco ransomware, pagare il riscatto o fare affidamento sui backup esistenti potrebbe non essere sufficiente a limitare i danni inflitti a un'entità dalla violazione informatica.

Secondo il Data Protection Trends Report, il 64% degli intervistati ha dichiarato di essere in grado di recuperare meno dell'80% dei propri dati dopo un attacco informatico, con circa un terzo dei dati non recuperabili.

Una buona pratica che un'entità può utilizzare per affrontare queste sfide è la regola del 3-2-1-1-0 quando si tratta della sua strategia di gestione dei dati. Assicurandosi di mantenere tre copie dei dati importanti, su almeno due diversi tipi di supporti, con almeno una di queste copie fuori sede; un backup dei dati fuori sede deve essere air-gapped, offline o immutabile, e che siano presenti zero errori a seguito di test automatizzati di backup e verifica della recuperabilità, i manager IT possono aiutare a proteggere meglio i loro dati da potenziali minacce ransomware.

Il Cyber Incident Reporting for Critical Infrastructure Act è un passo importante per aiutare a salvaguardare i settori istituzionali più importanti della nazione, aiutando ad avvertirli di minacce imminenti prima di un attacco.

Ma queste entità devono anche prendere misure per salvaguardare i loro dati ora per aiutare a mitigare i danni di una violazione informatica di successo.

Soci
Corporate

ALMAVIVA. Leader italiano nell'Information Technology, AlmavivA accompagna la trasformazione digitale nei settori chiave per l'economia del Paese.
La presenza in Italia come riferimento di valore. E da solide competenze Made in Italy, unite alla capacità di integrare culture, intelligenze ed esperienze diverse, è nato un network globale. Protagonista della trasformazione digitale.Tecnologie AI-driven «made in Italy» basate su Machine Learning, Deep Learning e Natural Language Processing. La Digital Transformation disegnata sulle frontiere dell'innovazione.
www.almaviva.it/it_IT

Aviogei, fondata nel 1970, è il principale produttore italiano di attrezzature dedicate all'assistenza aeroportuale. Progetta, assembla, certifica e distribuisce un'ampia gamma di prodotti per la movimentazione e il trasporto di passeggeri e merci, sia per uso civile che militare. È oggi presente in più di 180 aeroporti ed in 110 paesi nel mondo. Ha sempre prestato una particolare attenzione alla transizione energetica e alla mobilità sostenibile, a promuovere lo sviluppo della tecnologia in ambito automazione e controllo, collaborando con Enti di Ricerca e Università. Offre da anni attrezzature con batterie a litio di ultima generazione e forte è l'interesse dell'azienda a creare partenariati per realizzare soluzioni innovative. La produzione di Aviogei è rivolta anche alle macchine per la logistica aeronautica militare, alla quale è dedicato lo stabilimento di Dallas in USA per la progettazione dei mezzi elettrici.
www.aviogei.com

B.M.A. La B.M.A. nasce nel 1991 e fornisce supporto logistico ai reparti operativi delle Forze Armate, Polizia, Difesa Civile e SAR. Rappresenta in esclusiva in Italia società europee ed americane leader nel settore NVG e CBRN e fornisce consulenza ad aziende e gruppi aziendali sulle migliori strategie commerciali tramite: azioni di marketing, supporto pre e post vendita, partecipazione a gare e procedure pubbliche, realizzazione di corsi di formazione, traduzioni, gestione della codifica NATO, supporto in conferenze, incontri, meeting e seminari con stand, rappresentanza diretta e show-room di prodotti. Possiede la licenza T.U.L.P.S., art. 28 ed è certificata ISO 9001:2800.
www.bma-srl.it

Crisel srl fondata nel 1993, è una società leader nella commercializzazione di tecnologie, strumenti, apparati ad alto contenuto tecnologico per svariati ambiti: Spazio, Aerospazio, Difesa, Intelligence, Geospatial e GIS, Automotive e Ferroviario. Grazie alle competenze interne e alle rappresentanze internazionali è in grado di guidare il cliente verso la soluzione più adatta alle richieste di produzione e di ricerca. La nostra offerta si compone: Consulenza Tecnico Scientifica, System Design, Testing, Training, Distribuzione, Produzione, Vendita, Manutenzione e Postvendita. Soluzioni per Telemetria di bordo, Stazioni di terra e antenne telemetriche, Spazio, Geospatial Indoor e Outdoor, GNSS, Simulazione GNSS.
www.crisel.it

Crypt-Security è una PMI Innovativa che opera nell'ampio quadro di riferimento dell'Ecosistema delle Comunicazioni ed in particolare nel mercato della Sicurezza Informatica, settore che sta rivestendo sempre più una importanza strategica.
Grazie alla stretta collaborazione tra le attività di ricerca e l'interesse al mercato, Crypt-Security ha maturato competenze realizzative di altissimo livello nella progettazione e realizzazione di:

- Algoritmi di encryption-decryption;
- Sistemi di sicurezza;
- Soluzioni crittografiche;
- Consulenza sui temi della sicurezza, della probabilistica e della statistica applicata;
- Formazione sui temi della sicurezza.

www. crypt-security.com

Dassault Systèmes, the 3DEXPERIENCE Company, è catalizzatrice del progresso umano; mette ambienti virtuali in 3D collaborativi a disposizione di aziende e persone per concepire innovazioni sostenibili. Utilizzando la Piattaforma 3DEXPERIENCE ed i suoi applicativi per creare gemelli virtuali delle esperienze del mondo reale, i suoi clienti allargano i confini dell'innovazione, dell'apprendimento e della produzione. Dassault Systèmes genera valore per oltre 270.000 clienti di tutte le dimensioni e in tutti i settori industriali, in più di 140 Paesi.

www.3ds.com

Deimos Engineering si occupa dal 1996 di fornire servizi e software alle pubbliche amministrazioni e alle aziende private. Ha maturato dapprima una solida esperienza nella gestione ed elaborazione di dati geografici raster e vettoriali per poi sviluppare importanti competenze nella gestione, elaborazione ed analisi dei dati aziendali, nella creazione di sistemi evoluti di Business Intelligence e nella predisposizione di modelli previsionali avanzati basati sulle tecniche di Machine Learning. Deimos Engineering vanta importanti collaborazioni tecnologiche con la piattaforma per la Business Intelligence Tableau e con Rulex Inc, la più innovativa soluzione di Machine Learning sul mercato.
www.e-deimos.it

DigitalPlatforms SpA (DP) è un gruppo industriale italiano, in rapida crescita, che opera nel settore dell'Internet of Things, Cyber e delle tecnologie digitali.
Il Gruppo DP è composto da sette aziende/BU tutte basate in Italia, con una storia industriale compresa tra i 20 ed i 50 anni nel proprio settore di competenza.
DP è un player full liner, presente in tutti gli elementi necessari per realizzare soluzioni IoT end-to-end. DP parte dallo sviluppo, ideazione e produzione di sensori e prodotti di elettronica industriale, passando per i sistemi e le tecnologie di comando e controllo, fino alle piattaforme IoT, alla system integration IT e alla cybersecurity. Ciascuna delle aziende operative che fanno parte del Gruppo DP presidia uno dei diversi elementi della catena del valore della soluzione IoT/Cyber. DP si rivolge principalmente ai gestori di infrastrutture critiche in Italia ed all'estero, nei settori dell'energia, delle utilities, delle telecomunicazioni, dei trasporti e della Pubblica Amministrazione e Difesa.
www.platforms.it

Elettronica è una società all'avanguardia nel settore della Difesa elettronica e dello spettro elettromagnetico da 70 anni, fornisce ad oltre 30 Paesi nel mondo oltre 3000 sistemi di sicurezza per la difesa di piattaforme e di equipaggi in ogni dominio, compresi cyber e Spazio. L'azienda vanta un solido record di collaborazioni nazionali ed internazionali di successo su tutte le principali piattaforme militari moderne come il fighter Tornado, il caccia Eurofighter Typhoon, l'elicottero NFH-90, la piattaforma PPA italiana, le navi italiana e francese Horizon e FREMM, e una vasta gamma di progetti in diversi paesi in tutto il mondo.
Elettronica investe ogni anno 15 mln in R&S, ha oltre 1000 dipendenti e 6 sedi nel mondo. Certificata great place to work, Best Workplaces in Italia e in Europa, unica azienda della Difesa mai inserita in questa classifica. La società è capofila del Gruppo Elettronica a cui appartengono anche CY4GATE, società quotata, specializzata in Cyber EW, Cyber Security e Cyber Intelligence, è stata quotata di recente al mercato AIM con la quotazione IPO più importante degli ultimi 3 anni. Elettronica Gmbh, controllata tedesca, specializzata nella progettazione di sistemi di Homeland Security e EltHub, azienda del gruppo focalizzata su ricerca, innovazione e fast prototiping nei mercati adiacenti.
www.elt-roma.com

Esri Italia, Official Distributor di Esri per il mercato italiano, è l'azienda leader nelle soluzioni geospaziali, con sedi a Roma, Milano e Cagliari. Attraverso la sua offerta di prodotti e servizi, supporta Enti e Aziende nella trasformazione digitale, permettendogli di cogliere le opportunità offerte dalla "The Science of Where".
I nostri punti di forza:
• fornire ai Clienti la capacità di effettuare analisi geospaziali complesse sui propri dati;
• supportare Enti e Aziende nell'integrazione della componente geografica con le proprie piattaforme Enterprise;
• diffondere all'interno delle Organizzazioni la potenza della lettura geografica delle informazioni.
www.esriitalia.it

Eurelettronica Icas, fondata nel 1961, opera nel campo della progettazione, integrazione, vendita, installazione, assistenza tecnica, consulenza e formazione nell'ambito della Meteorologia e delle Scienze Atmosferiche, introducendo in Italia tecnologie innovative in vari settori applicativi. Sin dal 1979 è Rappresentante per l'Italia del gruppo Vaisala, per tutte le applicazioni di Meteorologia e dal 2011 Partner Tecnico Certificato. Da Novembre 2018 fa parte del gruppo Vaisala anche Leosphere, azienda già rappresentata da Eurelettronica Icas. E', inoltre, Distributore Esclusivo in Italia di: Kipp&Zonen, Totex, Millard Towers, Acams, Jotron. Tra i principali clienti: Aeronautica Militare, Esercito Italiano, Enav, ARPA Piemonte, ARPA Campania, ARPA Emilia Romagna, ARPA Veneto, ARPA Lombardia, ENEA, CNR, ENI Taranto, Autovia Padana, Autostrade per l'Italia, Iride Energia, ACTV, GDF Suez, JFCNP (NATO).
www.eurelettronicaicas.com

Fastweb offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese.
Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga. Fastweb ha sviluppato una rete nazionale in fibra ottica di 45.600 chilometri e oggi raggiunge con la tecnologia fiber-to- the-home o fiber-to- the- cabinet circa 7,8 milioni di abitazioni e aziende. Entro il 2020 Fastweb raggiungerà con la rete ultrabroadband 13 milioni di famiglie (ovvero il 50% della popolazione), di cui 5 milioni con tecnologia Ftth e velocità fino a 1 Gigabit e 8 milioni con tecnologia FttCab e velocità fino a 200 Megabit per secondo. La società offre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G e 4G Plus.
Entro il 2020 il servizio mobile verrà potenziato, a partire dalle grandi città, grazie alla realizzazione di una infrastruttura di nuova generazione 5G con tecnologia small cells.
La società fa parte del gruppo 18Swisscom dal settembre 2007.
www.fastweb.it

Forescout Technologies è il leader nelle attività di Device Visibility e Control. La nostra piattaforma di sicurezza unificata permette alle aziende e alle agenzie governative di ottenere una conoscenza completa e legata al contesto dell'ambiente relativo alla extended enterprise, includendo gli ambienti Campus, Data Center, Cloud, IoT e OT. Permette inoltre di coordinare le attività e le azioni dei sistemi di cybersecurity di terze parti presenti nell'infrastruttura aziendale al fine di ridurre i rischi operativi legati all'ambiente informatico e industriale.
I prodotti di Forescout Technologies possono essere istallati velocemente e permettono una operatività sia di tipo agentless che di tipo agent-based, e operano sia in modalità attiva che in modalità passiva a seconda delle esigenze e delle caratteristiche della infrastruttura di rete aziendale. Essi consentono, in tempo reale, la scoperta di ogni apparato connesso in modalità IP sull'infrastruttura di rete estesa, la classificazione intelligente e granulare degli stessi nonché la analisi posturale e lo stato dell'apparato individuato.
www.forescout.com

Fortinet rende possibile un mondo digitale di cui possiamo sempre fidarci attraverso la sua missione di proteggere persone, dispositivi e dati ovunque. Ecco perché le più grandi imprese, service provider e organizzazioni governative del mondo scelgono Fortinet per accelerare in modo sicuro il loro viaggio digitale. La piattaforma Fortinet Security Fabric offre protezione ampia, integrata e automatizzata sull'intera superficie di attacco digitale, proteggendo dispositivi, dati, applicazioni e connessioni critici dal data center al cloud fino all'home office. Al primo posto nella classifica delle appliance di sicurezza più vendute in tutto il mondo, oltre 580.000 clienti si affidano a Fortinet per proteggere le proprie attività. E il Fortinet NSE Training Institute, un'iniziativa della Training Advancement Agenda (TAA) di Fortinet, offre uno dei programmi di formazione più grandi e ampi del settore per rendere disponibili a tutti la formazione informatica e nuove opportunità di carriera.
www.fortinet.com

GMSPAZIO è attiva dal 2005 al servizio dei mercati dell'aerospazio, della difesa, della sicurezza nazionale e dell'ICT, con soluzioni tecnologiche di elevato livello focalizzate sulla gestione di scenari sintetici 4Ds (Spazio + Tempo) a supporto dei clienti per gestire: Scenari complessi di simulazione, Sorveglianza e Monitoraggio del traffico spaziale e Space Situational Awareness, Attività di Sorveglianza delle frontiere marittime, Modellazione delle reti di difesa missilistica, progetti di telerilevamento satellitare e attività di sorveglianza tramite UAV, offrendo prodotti, servizi e formazione per lo sviluppo di sistemi informativi integrati e personalizzati sulla base delle specifiche richieste degli utenti.
www.gmspazio.com

Hexagon è il gruppo leader mondiale nel settore delle soluzioni di realtà digitale che combinano sensori, software e soluzioni autonome. Ci avvaliamo dei dati per aumentare efficienza, produttività, qualità e sicurezza nell'ambito delle applicazioni industriali, manifatturiere, per le infrastrutture, il settore pubblico e la mobilità. Le nostre tecnologie modellano gli ecosistemi urbani e produttivi per renderli sempre più connessi e autonomi, garantendo un futuro scalabile e sostenibile. La divisione Safety, Infrastructure & Geospatial di Hexagon migliora l'affidabilità e la sostenibilità dei servizi e delle infrastrutture fondamentali. Le nostre soluzioni trasformano dati complessi su persone, luoghi e risorse in informazioni rilevanti. Le loro funzionalità permettono agli enti governativi e alle aziende del settore della difesa (anche pubblica), del trasporto e delle pubbliche utilità di prendere decisioni migliori e più veloci.
www.hexagongeospatial.com

I&C International Consulting S.r.l. è una società di ingegneria di Roma focalizzata sulla fornitura di servizi professionali per le organizzazioni che operano nell'ambito del Ministero della Difesa e della NATO. I servizi d'ingegneria coprono tutte le fasi del progetto, studi di fattibilità, progettazione, direzione lavori e collaudo nonché il supporto alla certificazione di infrastrutture con elevati requisiti di sicurezza. Le aree di competenza riguardano tutte le categorie di opere collegate alla Difesa, dai sistemi di telecomunicazione e radiocomunicazione agli impianti e opere civili. La I&C opera in conformità alle norme: ISO 9001, OHSAS 18001 e AQAP 2110.
www.intconsulting.it

IBM. Con più di 110 anni di storia, IBM è leader nell'Innovazione al servizio di imprese e istituzioni in tutto il mondo. Opera in oltre 170 paesi. L'azienda - una open hybrid cloud and AI platform company - offre alle organizzazioni di ogni settore l'accesso alle tecnologie esponenziali e ai servizi di consulenza per la trasformazione digitale e la modernizzazione dei modelli di business. Cloud ibrido, intelligenza artificiale, sistemi mainframe e storage, cybersecurity e quantum computing: queste le aree in cui IBM è riconosciuta come leader a livello globale e come brand dal forte impegno etico nei confronti del mercato e del contesto sociale in cui opera. IBM opera in Italia dal 1927. Tra i suoi clienti si possono annoverare i principali istituti bancari, le amministrazioni pubbliche e i leader di ogni settore industriale.
Per approfondire:
www.ibm.com/it-it/about

IES fondata nel 1990, è composta da un team di esperti nel campo dei sistemi di telecomunicazione per applicazioni civili e militari, negli ambiti terrestri, avionici, navali e ferroviari. La professionalità, la competenza e l'esperienza del proprio staff fanno della IES un interlocutore di primo piano, che la rendono fortemente competitiva nei settori strategici di prestigiosi enti pubblici, privati ed internazionali (NATO). Le attività principali riguardano: progettazione e realizzazione di innumerevoli prodotti (amplificatori RF, matrici Audio/RF, filtri, antenne), installazione e manutenzione di sistemi di comunicazione, con particolare attenzione allo sviluppo di specifici progetti per infrastrutture critiche ad alto livello di sicurezza.
www.iessrl.it

Keysight Technologies, Inc. (NYSE: KEYS) è un'azienda leader nel settore tecnologico che aiuta ad accelerare l'innovazione e connettere il mondo in modo sicuro. La dedizione di Keysight alla velocità ed alla precisione si estende anche alle analisi sul software che consentono l'introduzione di nuovi prodotti e sistemi elettronici sul mercato più rapidamente, con un'offerta che copre l'intero ciclo di vita del prodotto dalla simulazione progettuale alla validazione dei prototipi, al collaudo produttivo, fino ai test di performance e visibility delle reti e degli ambienti cloud. Le nostre applicazioni vengono utilizzate in ogni settore di mercato delle comunicazioni e dell'ecosistema industriale, nel settore aerospaziale e della difesa, automobilistico, energetico, dei semiconduttori e dell'elettronica generale. Nell'esercizio fiscale 2021, Keysight ha realizzato un fatturato di 4,9 miliardi di dollari. Maggiori informazioni sull'azienda sono disponibili all'indirizzo www.keysight.com, nella newsroom https://www.keysight.com/go/news e su Facebook, LinkedIn, Twitter e YouTube.
www.keysight.com

LARIMART S.p.A., società controllata da LEONARDO SpA, è un punto di riferimento pluridecennale nella progettazione e realizzazione di soluzioni e apparati in ambito Difesa, Sicurezza ed Emergenza. Ogni soluzione elettronica e di protezione personale Larimart nasce da un costante affiancamento agli utilizzatori finali e ai clienti. Dalla prima identificazione delle esigenze fino allo sviluppo, qualifica, fornitura e manutenzione, ogni dettaglio è ispirato a criteri di affidabilità e di evoluzione tecnologica. Larimart collabora con Agenzie Industrie Difesa per la realizzazione dei Giubbetti Anti Proiettile delle Forze Armate Italiane e ha recentemente acquisito la quota di maggioranza di DPI srl, azienda leader nelle protezioni per le vie respiratorie, consolidando la sua posizione come leader nazionale nel campo delle protezioni individuali.
www.larimart.it

Leonardo è un player globale ad alta tecnologia nei settori dell'Aerospazio, Difesa e Sicurezza. La Società progetta e realizza prodotti, servizi e soluzioni integrate per Governi, Forze Armate, clienti civili e istituzionali, coprendo ogni possibile scenario d'intervento: aereo e terrestre, navale e marittimo, spazio e cyberspazio. Leonardo, con sede in Italia, ha circa 50 mila dipendenti, una consolidata presenza industriale in quattro mercati principali (Italia, Regno Unito, Stati Uniti e Polonia) e un importante network di collaborazioni strategiche nei principali mercati mondiali ad alto potenziale. Ogni anno Leonardo investe in Ricerca e Sviluppo circa il 13% dei ricavi.
www.leonardo.com

National Instruments. Da oltre 40 anni NI accelera la produttività, l'innovazione e la scoperta attraverso una piattaforma aperta e basata sul software.
Questo approccio consente disviluppare e aumentare le prestazioni dei test e dei sistemi di misura automatizzati. I clienti di quasi tutti i settori, dall'Healthcare all'Automotive, dall'Aerospazio e Difesa all'Elettronica di Consumo e al mondo scientifico, utilizzano la piattaforma hardware e software integrata di NI per migliorare il mondo in cui viviamo, per superare le complessità delle sfide tecnologiche e le proprie aspettative. Con oltre 40 filiali presenti in tutto il mondo ed una base clienti di oltre 35000 aziende, National Instruments è l'azienda leader nel settore del test, della misura e del controllo automatici.
www.ni.com

Planetek Italia, da oltre 25 anni nel settore spaziale, partecipa ai principali programmi di osservazione della Terra e a numerose attività per la Difesa e la Sicurezza dell'Unione Europea. Le tecnologie sviluppate da Planetek sono state utilizzate nell'ambito di missioni spaziali duali, quali COSMO-SkyMed e COSMO-SkyMed Second Generation. Specifiche applicazioni di ultima generazione sono state sviluppate in partnership con la Hexagon Geospatial a supporto di IMINT e GeoINT per le FF.AA. Italiane, nell'ambito del programma nazionale di ricerca della Difesa, dimostrando il ruolo fondamentale delle tecnologie geospaziali in molte applicazioni, quali: supporto alle operazioni umanitarie; difesa dei confini; missioni militari internazionali.
www.planetek.it

Polomarconi.it S.p.A. società italiana con competenze specifiche nel settore delle comunicazioni a radiofrequenza con sedi a: Verona, Bergamo e Trento propone progetti di ricerca e sviluppo di sistemi a RF per i propri clienti nei settori ATC, LAND & NAVAL, TRANSPORT, PMR, DAS & 5G, M2M e MICROWAVE. I principali clienti di Polomarconi.it sono system integrators, produttori di radio e organizzazioni governative.
I sistemi offerti da Polomarconi.it per installazioni terrestri, aeree e navali includono combinatori multicanale automatici, filtri, accoppiatosi amplificati per la ricezione, duplexer, multiplexer, antenne e sistemi di antenne. Per i progetti più innovativi, Polomarconi.it collabora con istituti di ricerca e eccellenze universitarie in Italia e all'estero.
www.polomarconi.it

Serco Italia S.p.A. è la filiale italiana di Serco group Plc con sede nel Regno Unito ed é parte del dipartimento "Serco UK and Europe". Serco Italia ha oltre 40 anni di esperienza nel settore dello spazio e dell'Information Technology ed oltre 200 impiegati altamente qualificati nel settore spaziale. Considerando l' integrazione con le altre filiali in Europa, Serco ha una esperienza unica nel fornire supporto operativo ad organizzazioni quali:

- Organizzazioni internazionali (UE, Parlamento Europeo, BCE);
- Agenzie governative (ESA, ASI);
- Difesa (Esercito belga, Aeronautica Militare Italiana);
- Industria aerospaziale (Telesapazio);
- Istituzioni scientifiche (CNR, CERC);

Serco Italia offre soluzioni per l'intera gamma in ambito spaziale in Italia ed in Europa:

- Osservazione della Terra;
- Utilizzo dei dati Copernicus;
- Servizio Meteorologici;
- Scienze spaziali;
- Tecnologia;

www.serco.com

SIPAL S.p.A. Società leader nel settore dell'ingegneria, SIPAL SPA nasce nel 1978, per entrare nel gruppo FININC nel 1988. Con un know-how storico nel Supporto Logistico Integrato SIPAL si rivolge oggi al mercato civile e militare, con uno staff di oltre 400 professionisti ad altissimo tasso di specializzazione. Con 12 sedi in Italia e un'esperienza di oltre 40 anni, SIPAL lavora con flessibilità, rapidità e competitività, personalizzando in ogni dettaglio i servizi offerti. Dal 2018 SIPAL produce hardware e periferiche TEMPEST ed è diventata anche NATO BOA Partner; possiede altresì le abilitazioni necessarie per operare ai più elevati livelli di segretezza, supportando il cliente con una consulenza ad ampio spettro nella scelta dei sistemi più adatti alle singole esigenze. SIPAL è presente anche su scala internazionale, con snodi cruciali in India, Brasile, Romania, USA.
www.sipal.it

Studio Torta, leader nella consulenza della Proprietà Industriale, fornisce i più alti livelli di assistenza per la valorizzazione della creatività nel campo di brevetti, marchi e design, dalla fase delle ricerche preliminari al deposito delle domande di registrazione a livello nazionale e internazionale, dalla gestione nelle procedure amministrative all'assistenza nel contenzioso giudiziario. Fondato a Torino nel 1879, ha oggi uffici anche a Milano, Roma, Bologna, Treviso, Rimini. Lo Studio è strutturato come Società per Azioni con 60 professionisti, alcuni dei quali di madrelingua cinese, giapponese, tedesca e francese, specializzati per i mercati internazionali e circa 130 membri dello staff. Le competenze dei professionisti e il consolidato network di corrispondenti in tutto il mondo garantiscono un'assistenza puntuale nei più diversi settori industriali.
www.studiotorta.com

Teleconsys SpA, PMI innovativa, opera nell'ambito della consulenza, della integrazione di sistemi, dello sviluppo applicativo, della cybersecurity e della erogazione di servizi nel settore Information & Communication Technology, attraverso l'ideazione e la realizzazione di infrastrutture, applicazioni e piattaforme digitali innovative e l'erogazione di servizi specialistici ad alto valore aggiunto per la propria clientela di riferimento.
Teleconsys offre ai clienti competenze strategiche, consulenziali, tecnologiche, operative, condividendo le eccellenze presenti nel suo ecosistema dell'innovazione aperta per sviluppare, in maniera integrata, tutte le dimensioni necessarie per il successo di iniziative di innovazione digitale: cultura, persone, modelli di business, processi, tecnologie, ed operations.
www.teleconsys.it

Telespazio è tra i principali operatori mondiali nel campo dei servizi spaziali: dalla progettazione e sviluppo di sistemi spaziali, alla gestione dei servizi di lancio e controllo in orbita dei satelliti; dai servizi di osservazione della Terra, comunicazioni integrate, navigazione e localizzazione satellitare, fino ai programmi scientifici. Telespazio gioca un ruolo da protagonista nei mercati di riferimento facendo leva sulle competenze tecnologiche acquisite in 60 anni di attività, le proprie infrastrutture, la partecipazione a programmi spaziali come Galileo, EGNOS, Copernicus e COSMO-SkyMed. Telespazio è una joint venture tra Leonardo (67%) e Thales (33%); nel 2021 ha generato un fatturato di 605 milioni di euro e può contare su oltre 3000 dipendenti in nove Paesi.
www.telespazio.com

Thales Alenia Space. Da oltre quaranta anni Thales Alenia Space progetta, integra, testa e gestisce sistemi spaziali innovativi ad alta tecnologia per telecomunicazioni, navigazione, osservazione della Terra, gestione ambientale, ricerca scientifica e infrastrutture orbitali. Governi e industrie privati fanno affidamento su Thales Alenia Space per la progettazione di sistemi satellitari che provvedono in ogni luogo e in ogni momento alla connessione e al posizionamento, al monitoraggio del mostro pianeta, all'incremento delle sue risorse e all'esplorazione del nostro Sistema Solare e oltre.
Thales Alenia Space vede lo spazio come un nuovo orizzonte, aiutando a costruite una vita migliore e più sostenibile sulla Terra. Una Joint Venture tra Thales (67%) e Leonardo (33%), Thales Alenia Spaces Thales insieme a Telespazio forma la partnership strategica "Space Alliance", in grado di offrire un'insieme completo di servizi. Thales Alenia Space ha un fatturato consolidato di 2,15 miliardi di euro nel 2019 e 7.700 dipendenti nove paesi.
www.thalesaleniaspace.com

TS-WAY. Anno di fondazione 2010, un'expertise in cyber threat intelligence unica nel panorama italiano, TS-WAY sviluppa sistemi e tecnologie finalizzati alla produzione informativa per una difesa intelligence-driven. TS-WAY produce informazioni validate di tipo strategico, tattico operativo e tecnico, consentendo alle organizzazioni di risparmiare tempo e risorse, anticipare le minacce complesse e gli avversari strutturati, comprenderne la portata e la natura, potendo contare su un partner affidabile in caso di incidente informatico.
Un approccio alla sicurezza preventivo ed estremamente completo a garanzia e tutela dei beni e della continuità del business delle organizzazioni clienti.
www.ts-way.com

Vaisala, con più di 80 anni di esperienza, sviluppa e produce un'ampia gamma di sistemi, da sensori e stazioni meteorologiche automatiche, nefoipsometri, trasmissometri, visibilimetri/disdrometri, a sistemi di radiosondaggio e radiosonde, radar meteorologici in banda C e banda X, sistemi AWOS e per rilevamento Wind Shear. Grazie all'acquisizione di Leosphere, Vaisala è leader nel campo della fornitura di Lidar per monitoraggio dei campi di vento in diverse applicazioni. L'acquisizione dei servizi meteorologici B2B di Foreca rafforza lo sviluppo delle soluzioni nel campo digitale. Consistenti sono gli investimenti nello sviluppo delle tecnologie: Vaisala investe ogni anno fra il 10 e il 12% dei ricavi. Innovazioni sostenibili e basate sulla scienza sono valori fondanti. Vaisala è il partner ideale fornendo tutti i mezzi e gli strumenti affidabili e di alta qualità indispensabili per conoscere e gestire i fenomeni meteorologici e per sviluppare processi industriali sempre più sostenibili, assicurando la massima efficacia e sicurezza delle proprie attività.
www.vaisala.com

Vates is an Open Source software editor specialized in virtualization solutions. We develop in particular two software: XCP-ng (Xen Cloud Platform - new generation), a complete virtualization hypervisor that embeds its API and is based on Xen hypervisor. Xen Orchestra, on the other side, is a management interface that allows you to completely manage a virtual infrastructure based on XCP-ng or Citrix Hypervisor, from the creation and migration of VMs to the delegation of resources, including continuous replication and backup of VMs. Innovation is at the heart of our preoccupations and we invest considerably in R&D in order to improve the performance of our platforms, their security and thus be able to respond to emerging needs, particularly in terms of hybrid infrastructure and edge computing.
www.vates.fr

Veeam® è leader nelle soluzioni di backup, ripristino e gestione dei dati che offrono una Modern Data Protection. L'azienda fornisce un'unica piattaforma per ambienti Cloud, virtuali, fisici, SaaS e Kubernetes. I clienti Veeam hanno la certezza che le loro app e i loro dati siano protetti da ransomware, disastri e malintenzionati, e sempre disponibili grazie alla piattaforma più semplice, flessibile, affidabile e potente del settore. Veeam protegge oltre 400.000 clienti in tutto il mondo, tra cui l'81% della Fortune 500 e il 70% della Global 2.000. Veeam ha sede in Columbus, Ohio e ha uffici in oltre 30 Paesi. L'ecosistema globale di Veeam comprende oltre 35.000 partner tecnologici, rivenditori, fornitori di servizi e partner dell'alleanza e ha uffici in più di 30 paesi. Per saperne di più, visita https://www.veeam.com o segui Veeam su LinkedIn @veeam-software e Twitter @veeam.
www.veam.com

WiCode S.r.l. è un'azienda Italiana fondata nel 2015. In pochi anni ha raggiunto numerosi traguardi offrendo servizi e prodotti ad aziende pubbliche e private. Oggi è un punto di riferimento per la Cyber & Physical Security, CyberSpace, Social Resilience e Data Protection. Si avvale di professionisti specializzati e riesce a ricoprire ruoli sempre più all'avanguardia e complessi. Ha comprovata expertise nella progettazione, gestione e auditing in ambito Cyber & Physical Security nel settore ferroviario e infrastrutture critiche in genere.
WiCode attraverso i suoi Partner è presente in varie Nazioni Europee, negli USA e in America Latina. Aree di Intervento: Cyber Risk Assessment; Data Protection Plan; Social Engineering; Open Source Intelligence & Virtual HUMINT; ICT Resilience Auditing; Project Management; Blockchain; Virtual & Augmented reality; Smart Working.
www.wicode.it

AFCEA Capitolo di Roma
Via Arno 38, int. 9 Roma
tel +39 0694376483
fax +39 06 8845112
www.afcearoma.it

Il team editoriale ringrazia tutte le istituzioni civili e militari per il prezioso contributo fornito all'associazione.

Seguiteci anche su: