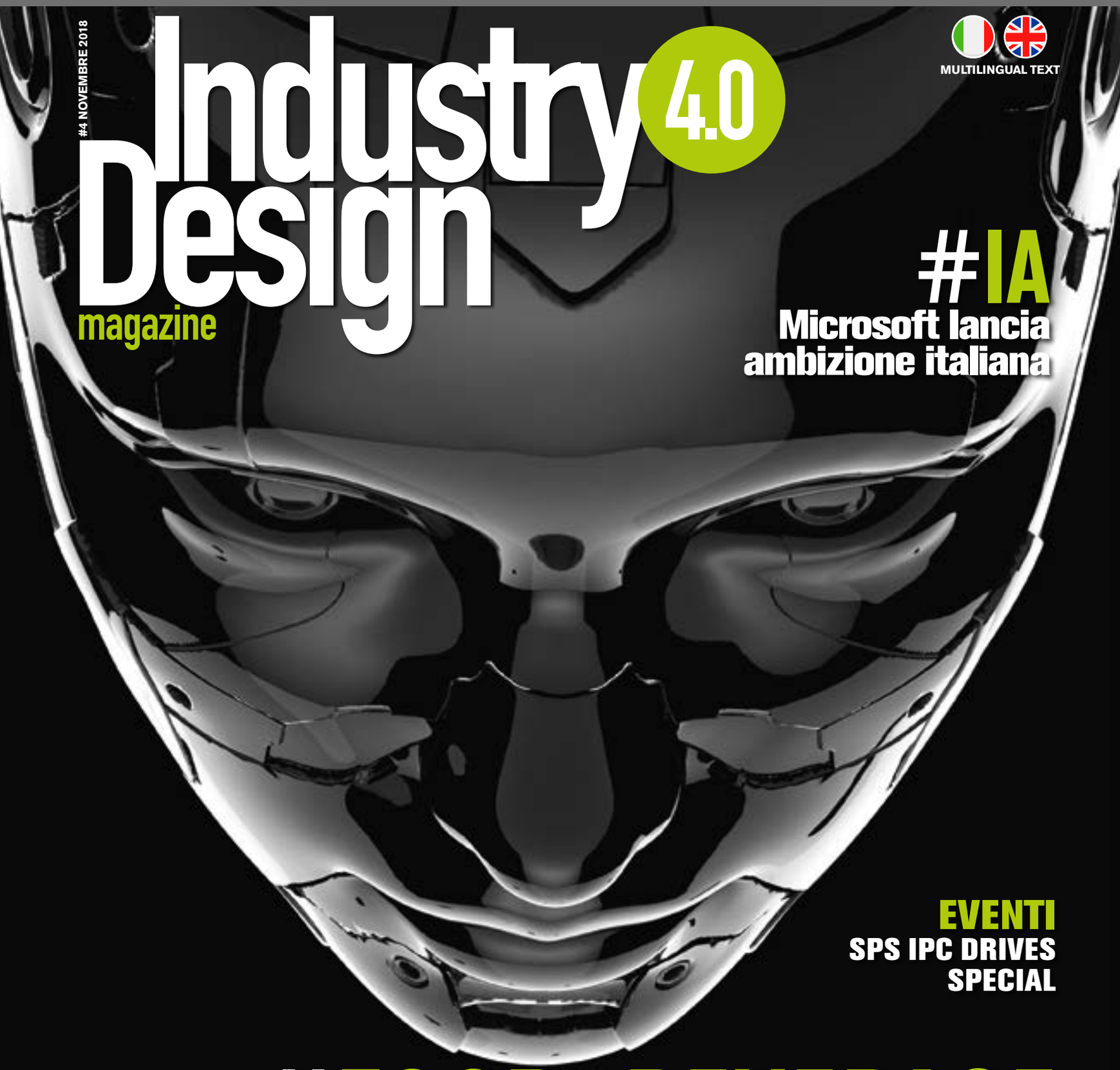
PRODUCTION | ENERGY | AUTOMOTIVE | PROCESS | PACKAGING

#4 NOVEMBRE 2018

Industry 4.0 Design magazine

MULTILINGUAL TEXT

#IA
Microsoft lancia ambizione italiana



EVENTI
SPS IPC DRIVES SPECIAL

#FOOD&BEVERAGE
GARANTIRE SICUREZZA, QUALITÀ E TRASPARENZA ATTRAVERSO LA TECNOLOGIA

Quine Business Publisher

Industrial IT solutions

di Cristian Randieri, membro del Comitato Italiano per l'Ingegneria dell'Informazione C3i delegato dell'Ordine degli Ingegneri di Siracusa.

LA COMUNICAZIONE VIA SATELLITE PER LA BUSINESS CONTINUITY ED IL DISASTER

E' ormai un dato di fatto che le moderne applicazioni IT non possono più prescindere dalla rete mediante la quale sono garantiti i collegamenti a sedi remote, i software gestionali centralizzati, la posta elettronica, le operazioni bancarie, le applicazioni CLOUD, i sistemi IoT, e così via.

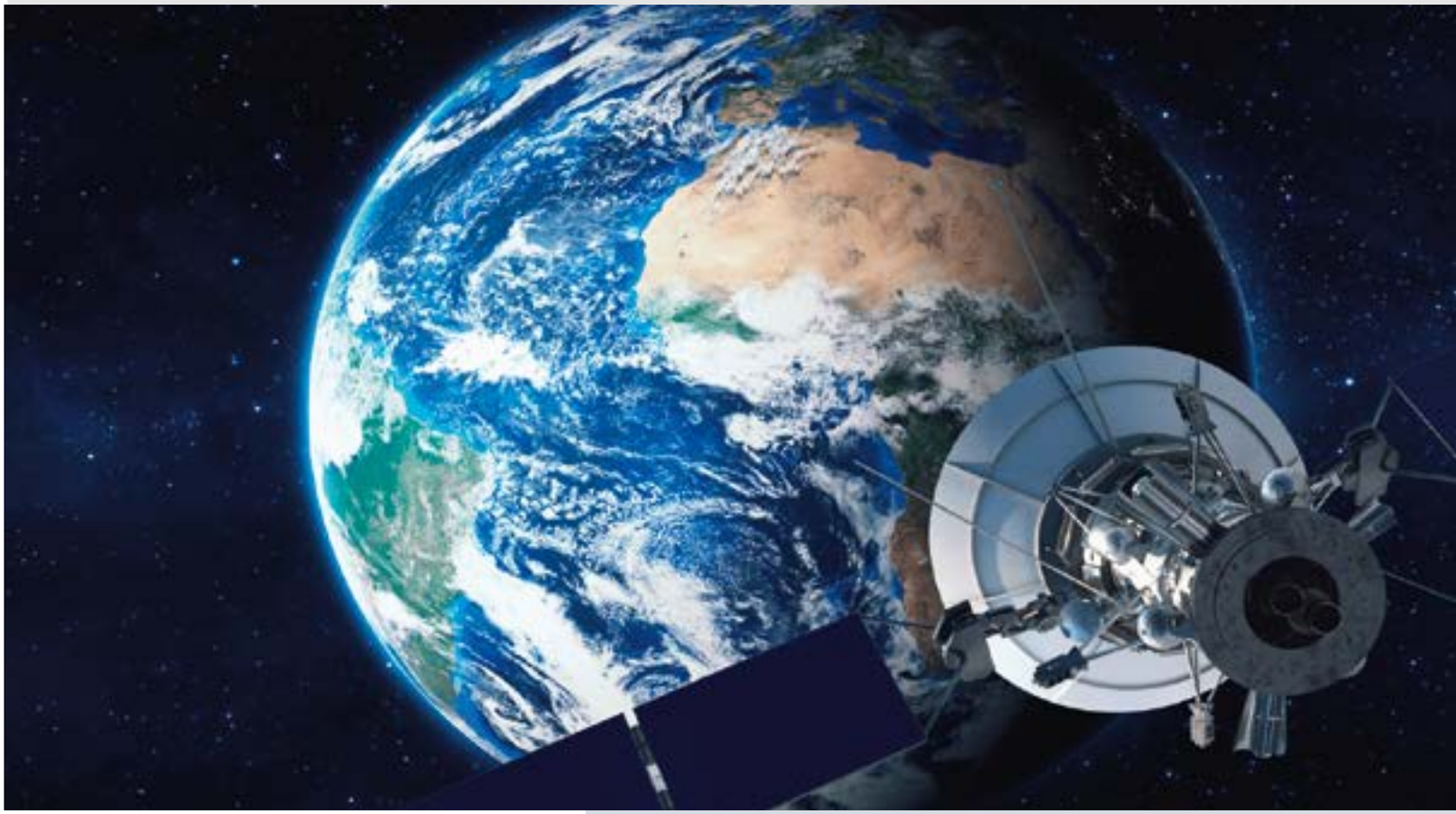
Purtroppo alla crescente domanda di servizi e traffico di rete non è seguita un'analoga crescita delle relative infrastrutture, tantoché l'attuale ecosistema Internet non è più sostenibile a causa di un traffico dati sempre più gravoso, per lo più generato da applicazioni e servizi fondamentali per ogni azienda. In pochissimo tempo è variato notevolmente l'utilizzo della rete, passando da un sistema che sino a qualche anno fa si basava sulla trasmissione di testi ad un sistema con una forte componente multimediale, circostanza che ha causato un aumento indiscriminato del traffico dati caratterizzato dallo scambio di file multimediali di grandi dimensioni. Sfortunatamente questa mole di traffico è destinata crescere sempre più negli anni, rendendo necessari nuovi investimenti in infrastrutture che tardano a venire, di conseguenza la quasi totalità della rete è oggi gestita in modalità "Best Effort"; ossia la maggior parte degli operatori di telecomunicazione Italiani (ma anche esteri) non garantiscono il loro servizio offerto in termini di interruzione di servizio (cadute di rete). E' anche vero che la minoranza di essi contrattualizza secondo il concetto di SLA (Service Level Agreement), garantendo al cliente un risarcimento indipendentemente dal danno subito in caso di disservizi della rete. Malgrado ciò nella maggior parte dei casi il danno subito supera di gran lunga in mero risarcimento offerto dall'operatore. Anche il tempo d'intervento di un operatore non po' essere valutato a priori perché il controllo della rete è frammentato spesso tra i diversi operatori. Tutte queste complessità ci fanno capire che nella maggior parte dei casi i tempi di risoluzione dei problemi saranno certamente più lunghi di quelli che la nostra attività aziendale si può permettere.

Quando si parla di disaster recovery e business continuity di norma ci si riferisce a quelle tecniche che assicurano la capacità aziendale nel continuare ad esercitare il proprio business a fronte di eventi avversi che possono colpirla. In particolare oggi la tecnologia offre la possibilità di realizzare varie soluzioni di continuità e Disaster Recovery atte a garantire l'erogazione continua dei servizi IT definiti col termine "mission critical". La business continuity occupandosi della pianificazione della continuità operativa e di servizio è responsabile del

ENGLISH TEXT

ABSTRACT:

The Internet not only constitutes the most powerful means of communication at our disposal, it has become the very foundation for virtually any type of business today. Thus, using the best technologies available on the market to protect personal data – involving aspects of both Business Continuity and Disaster Recovery in accordance with the GPDR – is absolutely essential. Data transmission via satellite is useful in critical situations calling for a maximum of reliability and redundancy in data communication. The current explosion of global Internet traffic is due in large part to modern IT applications, the widespread availability of broadband connections and the increasing dissemination of multimedia content, so our objective for the future must be to invest in improving infrastructure with higher performance networks to ensure better accessibility.



ripristino dei processi aziendali essenziali anche in caso di eventi disastrosi che hanno una probabilità molto bassa di accadere, ma le cui conseguenze possono essere estremamente gravose per il business.

Mediante la definizione del Business Continuity Plan (BCP) devono essere identificati i pericoli potenziali che minacciano l'organizzazione; suggerendo e fornendo una struttura che consente di aumentare la capacità di adattamento alle condizioni d'uso con una capacità di risposta la più veloce possibile; in maniera da salvaguardare gli interessi delle parti in causa, le attività produttive, l'immagine, riducendo i rischi e le conseguenze sul piano gestionale, amministrativo e legale.

In pratica, di norma i sistemi e i dati considerati "primari" vengono ridondati in un sito secondario denominato "Disaster Recovery Site" per far sì che in caso di disastro tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile ripristinare le attività sul sito secondario nel più breve tempo e con la minima perdita di dati possibile.

Per ottemperare a ciò i manager delle medio-grandi aziende e grandi aziende guardano sempre più le problematiche della sicurezza informatica con occhi diversi cercando sempre di trovare nuove soluzioni tipicamente basate su componenti hardware e software ma difficilmente viene preso seriamente in considerazione il caso più estremo in cui possa avvenire una catastrofe naturale per cui si ha il cedimento di tutte le infrastrutture terrestri di comunicazione. Tutti quanti sperimentiamo banalmente il collasso delle reti cellulari nei minuti che precedono e susseguono la mezzanotte di ogni nuovo anno. In questi minuti è quasi impossibile riuscire a comunicare con un altro interlocutore a cause del sovraccarico delle linee che non sono progettate per gestire una così grande moltitudine di comunicazioni simultanee. Se adesso per un attimo provassimo ad immaginare un caso concreto di calamità naturale ecco che ci rendiamo subito conto di quanto siano vulnerabili i nostri sistemi di comunicazione. Anche se alcune compagnie stanno seriamente studiando polizze assicurative specifiche, al momento non esistono assicurazioni che possano coprire i danni provocati da un attacco informatico e tanto meno da una evento catastrofico, sia esso naturale che ad opera dell'uomo, che metta in ginocchio tutti i sistemi di telecomunicazioni comunemente adoperati quali ad esempio internet e la telefonia sia essa fissa che mobile.

D'altro canto anche l'art. 32 del GDPR che si occupa nello specifico della sicurezza del trattamento dei dati

personali ("Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio") ci ricorda che quest'ultima dovrà essere garantita attraverso l'adozione di una serie di misure concrete. Secondo questa norma, infatti, il titolare e il responsabile del trattamento dei dati personali dovranno predisporre ed attuare delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.

Più nello specifico, alcune delle misure che il titolare o il responsabile del trattamento dei dati potranno concretamente adottare sono, come stabilito dall'art. 32, paragrafo 1:

1. la pseudonimizzazione e la cifratura dei dati personali;
2. la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
4. una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In particolare il punto 3. attribuisce rilievo anche al concetto di disaster recovery, che come già detto, consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento.

Considerando che le misure richieste sono improntate sulla tutela dei diritti di privacy, è evidente che tali misure coinvolgono molti degli aspetti operativi della maggior parte delle aziende strettamente legati alla connettività. Qualora infatti il back-up periodico, non possa aver luogo, per motivi di connettività dovuti a disastri (ad esempio alla gestione cloud di database remoti), qualsiasi azienda si troverebbe con le proprie informazioni non allineate. Ne consegue che è importantissimo, anche dal punto di vista giuridico, premunirsi contro il rischio di perdita dati anche in caso di disastri. Per far ciò unitamente ai sistemi di memorizzazione è d'obbligo ridondare anche la connettività.

Ridondare le infrastrutture di rete terrestri con altre terrestri, è una soluzione da scartare in caso di disastri poiché anche se le linee dati sono differenziate è molto probabile che un terremoto o una inondazione possa mettere fuori servizio tutte le centrali della zona; indipendentemente dall'operatore che le gestisce. La stessa cosa vale anche per tutte le reti wireless (siano esseWi-Fi che cellulari) che poggiano su infrastrutture terrestri (la quasi totalità). Poiché le catastrofi possono verificarsi inaspettatamente in qualsiasi momento, ed ovunque, la capacità aziendale di mantenere in essere le comunicazioni dati in queste situazioni di criticità è una chiave di successo per mantenere in vita una complessa infrastruttura IT aziendale. All'occorrenza di una catastrofe è richiesto un team di persone esperte nel campo delle telecomunicazioni che siano in grado di mantenere in funzione tutti i sistemi IT aziendali. Ad oggi la soluzione via satellite è l'unica che garantisce una la continuità delle telecomunicazioni, anche nei casi più drammatici, fornendo un servizio di ridondanza ed implementabile in pochissimo tempo. Tutto ciò grazie al fatto che il mondo delle connessioni dati Satellitari è molto cambiato; sino a qualche tempo fa gli elevati costi ne permettevano il loro utilizzo solo per applicazioni prettamente militari. Il lancio di nuovi satelliti e l'innovazione tecnologica degli ultimi giorni hanno permesso l'incremento delle prestazioni proporzionale ad un notevole abbassamento dei costi inerenti i servizi ad essi connessi, permettendo la loro diffusione in ambiente sia industriale che civile. Grazie alle nuove flotte di satelliti geostazionari, in orbita a circa 36.000 km dalla Terra, la connessione satellitare «bidirezionale» è in grado di offrire collegamenti alla rete ad alta velocità in qualunque zona del globo, a patto che sia possibile un allacciamento del sistema ad una fonte di energia. Con i recenti satelliti lanciati alla fine del 2013, la connessione satellitare è diventa addirittura tecnicamente competitiva rispetto alle attuali connessioni terrestri in fibra ottica.

I satelliti ricevono e inviano dati alle antenne ricetrasmittenti installate presso il cliente e li ritrasmettono a grandi infrastrutture connesse alle dorsali in fibra ottica, denominate Teleporti, dislocate in tutto il globo. Grazie a questi ultimi è possibile «prolungare» a largo raggio le comunicazioni internet, dati e voce, offrendo servizi ad alto valore aggiunto: dall'ultimo miglio bidirezionale alla creazione di reti di distribuzione di contenuti, alle connessioni ad Internet a banda larga, alla realizzazione di reti private (VPN), fino all'emissione di segnali radiofonici e televisivi.La ridondanza satellitare è sicuramente uno dei temi che debbono essere affrontati nel BCP di ogni azienda poiché ogni satellite funziona senza alimentazione terrestre; l'unica alimentazione da garantire è quella del modem installato a terra (a bassissimo consumo, e quindi alimentabile con sistemi UPS e batterie tampone). Tutte queste caratteristiche garantiscono la ridondanza a livello di sistema, estrema flessibilità e scalabilità unitamente ad una rapida implementazione. In conclusione possiamo affermare che la tecnologia satellitare, grazie alla sua fisicità, è attualmente il sistema di telecomunicazione più sicuro poiché meno attaccabile e intercettabile da pirati o vandali (motivo per cui è ampiamente usato in ambito militare). ■