



Ministero delle Imprese e del Made in Italy

DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE

SCUOLA SUPERIORE DI SPECIALIZZAZIONE IN TELECOMUNICAZIONI

PROGRAMMA

Anno accademico 2023/2024

Corso di **TELEFONIA E TELEGRAFIA**

Modulo di **NETWORK PROGRAMMABILITY**

Ore previste: **30**

OBIETTIVI DEL CORSO

Il modulo mira ad introdurre le tecnologie e le tecniche abilitanti alla creazione di una rete programmabile, sia sui piani di gestione e controllo che sul piano dei dati. Inoltre viene fornita una panoramica dei casi d'uso più rilevanti che beneficiano della (o che sono abilitati dalla) disponibilità delle reti programmabili.

PROGRAMMA

- Richiami di networking
 - architettura di rete
 - metriche prestazionali
 - modello ISO/OSI
- Network Automation
 - NETCONF e RESTCONF
 - Data Modeling Languages e YANG
 - esempi applicativi
- Control Plane Programmability
 - Software Defined Networking
 - Openflow
 - esempi applicativi
- Network Softwarization
 - ETSI use cases
 - Network Function Virtualization
 - NFV placement
 - Service Function Chaining e Network Service Header
 - SRv6
- Data Plane Programmability
 - Programmable Devices
 - P4 Language
 - esempi applicativi



Modulo di **SICUREZZA NELLE COMUNICAZIONI**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo mira a fornire gli elementi concettuali e tecnici di base per la comprensione dello stato dell'arte nelle comunicazioni sicure, a definire la terminologia tecnica relativamente agli elementi introduttivi di crittografia e protocolli di comunicazione sicuri ed a fornire elementi di base sulla valutazione della sicurezza di algoritmi e protocolli.

PROGRAMMA

- Introduzione alla sicurezza nelle comunicazioni
- Introduzione alla crittografia
- Primitive crittografiche: cifratura e autenticazione di messaggio a chiave simmetrica
- Cifratura e autenticazione di messaggio a chiave pubblica (RSA). Cenno alla crittografia basata sulle curve ellittiche
- Autenticazione di identità: classificazione, definizioni. Password
- Autenticazione su base indirizzo
- Protocolli crittografici: caratteristiche principali e attacchi
- Protocolli di autenticazione: sfida-risposta, Needham-Schroeder
- Protocolli di autenticazione e scambio chiavi (instaurazione di un canale sicuro): Diffie-Hellman autenticato
- Autenticazione su base password forte: Lamport hash, EKE, SRP
- Condivisione dei segreti
- IPSec e IKE

Modulo di **CODIFICA E AFFIDABILITÀ**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo si prefigge di riassumere le basi di telecomunicazioni e l'acquisizione degli elementi base della protezione dell'informazione e impatto a livello di sistema.

PROGRAMMA

- Scenari Evolutivi delle TLC
Sistemi di accesso cablato e wireless
Sistemi cellulari e comunicazioni a corto raggio (NFC, Bluetooth)
Radio Cognitiva
- Il problema della codifica di sorgente
Sorgenti discrete stazionarie senza memoria
Compressione ottima secondo Huffman
Sorgenti discrete e stazionarie con memoria
Sorgenti di Markov
- Il problema della codifica di canale e la contrapposizione tra affidabilità e velocità trasmissiva
Codifica a Blocchi
Decodifica MV
Decodificatore a Sindrome
- Codifica convoluzionale. Utilizzo del meccanismo di memoria
Algoritmo di Viterbi in modalità Hard e Soft. Interleaving
- Meccanismo ARQ per la protezione da errori. Protocolli Stop and Wait, Go Back n, selective repeat



Modulazioni numeriche. Modulazioni PAM e QAM

- Modulazione OFDM nella versione analogica e digitale
- Schemi di accesso a suddivisione di canale. TDMA, FDMA e CDMA
Schemi di accesso a contesa: Slotted Aloha e CSMA nelle versioni Collision Detection e Collision Avoidance



Corso di **RADIOTELEGRAFIA E RADIOTELEFONIA**

Modulo di **ANALISI DEL FUNZIONAMENTO DEI MODERNI SISTEMI RADIOMOBILI**

Ore previste: **30**

OBIETTIVI DEL CORSO

Obiettivo del modulo è quello di fornire una descrizione dei concetti generali e delle metodologie alla base dell'analisi del funzionamento dei moderni sistemi radiomobili. Nella presentazione degli argomenti trattati si focalizza l'attenzione sui problemi generali riguardanti la realizzazione di un moderno sistema radiomobile. Per ciascuno dei problemi analizzati sono descritte le relative soluzioni implementate nei sistemi 4G, 5G e nei futuri sistemi 6G. I principali argomenti presentati nel corso riguardano: 1. l'analisi delle architetture delle moderne reti radiomobili; 2. il problema di ottimizzazione del throughput mediante tecniche di caching e di edge cloud computing; 3. l'organizzazione delle moderne reti radiomobili con particolare riferimento ai sistemi 4G LTE e 5G.

PROGRAMMA

- Concetti generali sui sistemi radiomobili e visione di alto livello. Organizzazione cellulare della sezione di accesso. Concetto di cluster e tecniche di settorizzazione. Parametri che qualificano le prestazioni di un sistema radiomobile
- Gestione della mobilità e funzionalità di handover. I servizi radiomobili e loro evoluzione. Distinzione tra servizi portanti e teleservizi. Importanza dei nuovi servizi basati sulla trasmissione dati. La classificazione ITU dei servizi introdotta per il 5G
- I moderni sistemi radiomobili: concetti generali. Evoluzione della rete di accesso radio orientata al miglioramento della efficienza spettrale di sistema. Problema della latenza nei sistemi radiomobili. Architetture di rete di accesso a salto singolo o salto multiplo, reti mesh e loro impieghi nelle moderne reti di accesso radio
 - La formula della capacità di Shannon e sue implicazioni nel progetto delle moderne reti di accesso via radio. Uso efficiente dello spettro radio. Concetto di spectrum sharing per le reti di nuova generazione
 - Le reti di accesso di tipo eterogeneo. Dispiegamento di una rete eterogenea. I capacity boosters. Micro, pico e femtocelle. Tecniche per la gestione della interferenza: ICIC, eICIC e note sul COMP
- MIMO. Concetti Generali. Tipologie di MIMO: SU-MIMO, MU-MIMO e Massive MIMO
- Evoluzione delle architetture delle reti radiomobili: dalla RAN passando per la Cloud RAN fino alla OpenRAN
- Concetti di: QoS, QoE e TCP Throughput (Formula di Matis). Uso di piattaforme di QoE per il miglioramento delle prestazioni nelle moderne reti di Telecomunicazione. Lo Edge Cloud Computing e il Multi Access Edge Computing
- Evoluzione dei sistemi radiomobili. Dal 2G al 4G passando per il 2.5G e il 3G
- Il sistema 4G LTE
 - Architettura generale ed entità funzionali: eNB ed EPC. Separazione delle funzionalità del piano di controllo (MME, PCRF, P-GW etc.) e di utente e sue implicazioni (S-GW, P-GW)



- Architettura protocollare del LTE: piano di controllo e piano di utente. Concetto di EPS bearer. Descrizione di dettaglio delle funzionalità di alcuni strati protocollari del sistema LTE
- Interfaccia radio del LTE: OFDM e SC-FDMA. Cenni sulla tecnica OFDM. Assegnazione delle risorse nel LTE: il physical resource block (PRB) e il resource block (RB). Valutazione del data rate ottenibile sulla interfaccia radio LTE
- Brevi cenni sul 5G: percorso di standardizzazione e stato attuale dello sviluppo. Architettura di rete 5G ed elementi che realizzano i piani di utente e di controllo. Confronto architettura di rete 4G e 5G e innovazioni introdotte nel 5G. Descrizione di dettaglio della interfaccia radio del 5G: lo Scalable-OFDM e numerologia

Modulo di

LTE, LTE AVANZATO ED INTRODUZIONE AL 5G

Ore previste:

10

OBIETTIVI DEL CORSO

Obiettivo del modulo è quello di fornire una presentazione dei sistemi radiomobili di 4^a e 5^a generazione, di descrivere le tecniche realizzate per ottenere elevato data rate e connettività di molti dispositivi contemporaneamente e le tecniche per ottenere una bassa latenza.

PROGRAMMA

- LTE (completamento)
 - Tecnica Orthogonal Frequency Division Multiplexing (OFDM)
 - Accesso multiplo e Strato fisico LTE parte 1 (physical resource block, organizzazione della trama)
 - Strato fisico LTE parte 2 (canali fisici/trasporto, procedure di trasmissione dati)
 - Strati MAC, RLC e PDCP
 - Strato RRC e cenni sul NAS
 - Esempio di procedura Initial Attach
- LTE ADVANCED
 - Tecnica MIMO
 - Carrier Aggregation
 - Small Cell
 - Dual Connectivity
- Introduzione al 5G
 - Use case del 5G e visione architetturale
 - Tecnologie principali del 5G
 - Architettura: dual connectivity, Network slicing, radio cloud edge computing
 - Strato fisico 5G (new radio e numerology), innovazioni sull'interfaccia radio 5G (minislot, self-contained frame, canali di controllo)



Corso di **COMMUTAZIONE E SEGNALAZIONE**

Modulo di **CONFIGURAZIONE E GESTIONE RETI TCP/IP**

Ore previste: **30**

OBIETTIVI DEL CORSO

L'obiettivo formativo del modulo è quello di fornire allo studente le conoscenze teoriche e pratiche (basate su Linux) di networking TCP/IP che gli permettano di gestire e progettare ambienti d'ufficio centralizzati o distribuiti (smart working).

PROGRAMMA

- Richiami TCP/IP, indirizzamento e forwarding
- Configurazione sperimentale ed analisi di reti IP su Linux in ambiente GNS3
- Teoria e laboratorio dei servizi di Network Address Translation (DNAT, SNAT) e DHCP
- Teoria e laboratorio dei servizi di DNS
- Teoria e laboratorio dei servizi di Proxy (forward, reverse)
- Richiami Sicurezza TLS
- Teoria e laboratorio di Virtual Private Networks basate su TLS

Modulo di **FONDAMENTI RETI IP**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo ha l'obiettivo di illustrare il funzionamento delle reti IP analizzando il comportamento nei principali livelli OSI, dallo strato fisico a quello di trasporto. In particolare si analizzeranno le reti Ethernet, i processi di routing, la gestione della qualità dell'informazione sino alla valutazione delle prestazioni. Il corso verrà inquadrato nell'ambito delle ultime metodologie delle reti basate sui paradigmi SDN e NFV a supporto delle reti 5G.

PROGRAMMA

- Introduzione alle reti IP
 - Dalle reti NGN alle reti 5G
 - Criteri SDN e NFV
 - Il modello OSI
- OSI Layer 1
 - Dal PDH a SDH
 - OTN
- OSI Layer2
 - 802.3
 - Reti Ethernet, GbE
 - Switch, Spanning Tree
 - Virtual LAN
- OSI Layer3
 - Protocollo IP, struttura del pacchetto
 - ICMP
 - Ping e traceroot
- Indirizzamento e routing
 - NAT, DHCP, supernatting



-
- Cenni BGP e EGP
 - OSI Layer 4
 - TCP e UDP
 - TCP
 - Controllo d'errore, fast retransmit
 - Controllo di flusso e congestione
 - Principali TCP (Tahoe, Rino, New Rino, Cubic)
 - Cenni IPv6
 - Prestazioni reti IP
 - Intserv e Diffserv
 - QoS, throughput
 - Misura QoS, multisessione
 - Cenni Reti IP Mobile e Multimediali
 - SIP, IMS, VoLTE
 - IP mobile
 - Cenni sicurezza quantistica (Quantum Key Distribution)
 - Sicurezza adottata nei livelli OSI



Corso di **ENERGETICA E PROBLEMI DI TERMODINAMICA**

Modulo di **ENERGETICA**

Ore previste: **30**

OBIETTIVI DEL CORSO

Il modulo si prefigge l'obiettivo di presentare il quadro attuale del settore energetico nazionale ed internazionale con l'individuazione a livello nazionale del quadro normativo, dei meccanismi di regolazione ed incentivazione previsti nel settore delle energie rinnovabili e dell'efficienza energetica.

PROGRAMMA

- Il quadro normativo
- Le diagnosi energetiche
- Data center
- I meccanismi di incentivazione
- Il meccanismo dei titoli di efficienza energetica
- Il conto termico
- Il PREPAC
- Casi studio e applicazioni pratiche
- Impianti a fonti rinnovabili
- Interventi di efficientamento energetico
- Bilancio di sostenibilità
- Analisi delle emissioni dei gas climalteranti
- Footprint Scope 1, Scope 2, Scope 3



Corso di **IMPIANTI DI TLC**

Modulo di **SISTEMI E RETI WIRED**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo ha l'obiettivo di illustrare il funzionamento completo delle reti fisse sia in fibra ottica che in doppino a livello fisico. In particolare il corso si focalizzerà sui sistemi ottici dal trasmettitore al ricevitore, considerando i limiti imposti dalle fibre ottiche e da altri dispositivi presenti nelle reti, e si analizzeranno le prestazioni sia dei sistemi (sia IM-DD che coerenti, singolo canale e WDM) che delle relative reti. Particolare attenzione verrà data alle reti di accesso ottiche (FTTx, PON) e alla loro integrazione con le reti 5G. E' previsto anche un laboratorio virtuale basato sull'utilizzo di un codice che simula le prestazioni dei sistemi ottici e che permette la progettazione di una rete.

PROGRAMMA

- Introduzione ai sistemi ottici
 - Shannon
 - Reti ottiche
- Cenni laser, fibre ottiche, fotodiode
- Sistemi IM-DD
 - Rumore Shot e termico
 - Calcolo probabilità di errore, fattore Q
 - Amplificatore ottico e limite quantico
- Sistemi coerenti
 - FSK, PSK, ASK
 - M-QAM
 - OFDM
- Sistemi Sub-Carrier Multiplexing
 - CATV
- Sistemi xDSL
 - Banda doppino telefonico
 - DMT
 - Vectoring
- Reti di accesso
 - FTTx
 - PON, EPON, GPON, WDM-POB
 - Costi rete di accesso
 - Reti ottiche per 5G (Backhauling, FrontHauling)
- Reti di Edge e core
 - OXC, OADM
- Laboratorio virtuale di reti ottiche
 - Codice di simulazione
 - Test sistemi IM-DD
- Sicurezza reti ottiche
 - Attacchi in reti ottiche
 - Cenni sulla sicurezza quantistica (Quantum Key Distribution)



Corso di LEGISLAZIONE ED ECONOMIA

Modulo di DIRITTO E POLITICHE DEL CYBERSPAZIO PER LA SICUREZZA NAZIONALE

Ore previste: 10

OBIETTIVI DEL CORSO

L'obiettivo è quello di fornire ai partecipanti una overview completa delle principali normative europee e nazionali in materia di cybersecurity e di sicurezza e difesa dello spazio.

PROGRAMMA

- La Cyber Strategy dell'Unione europea
 - I pilastri strategici europei
 - Il ruolo delle norme nella cyber strategy europea
 - Gli obiettivi a supporto del settore delle telecomunicazioni
- La Direttiva NIS 2
 - Dalla Direttiva NIS alla Direttiva NIS 2
 - Le richieste del legislatore europeo
 - Gli obblighi di *compliance*
- Il Cybersecurity Act e Il Cyber Resilience Act
 - Il quadro europeo di certificazione della cybersicurezza
 - Il quadro giuridico sui requisiti essenziali di cybersicurezza per l'immissione sul mercato di prodotti con elementi digitali
 - L'interazione tra le due normative e il restante quadro giuridico europeo
- La Strategia Nazionale di Cybersicurezza 2022 – 2026
 - I pilastri strategici nazionali per la cybersicurezza
 - Il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN)
 - I pilastri tecnico-operativi
- Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)
 - Gli obiettivi del legislatore italiano
 - L'impianto normativo a tutela della sicurezza nazionale
 - Gli obblighi di *compliance*
- La Strategia spaziale dell'Unione europea per la sicurezza e la difesa
 - Gli attacchi da cyberspazio a spazio e da spazio a cyberspazio
 - L'impianto strategico per la sicurezza e difesa dello spazio
 - L'azione del governo italiano

Modulo di CYBERSICUREZZA NAZIONALE: CERTIFICAZIONI, ISPEZIONI, INTERNET GOVERNANCE

Ore previste: 5

OBIETTIVI DEL CORSO

L'obiettivo formativo è di fornire il quadro d'insieme degli aspetti di vigilanza, ispezione e certificazione nei settori volontari e cogenti relativi alla cybersicurezza.



PROGRAMMA	<ul style="list-style-type: none">• Organismo di Certificazione della Sicurezza Informatica• Organismo di ispezione - Attività ispettive previste nella normativa per la cybersicurezza nazionale.<ul style="list-style-type: none">○ Attività ispettiva per l'accreditamento dei laboratori di valutazione della sicurezza dell'OCSI○ Attività ispettiva per l'accreditamento dei laboratori di prova del Centro di valutazione e di certificazione nazionale (CVCN)• Internet Governance D.P.C.M.19 giugno 2019, n. 93 (art. 10 lettera r)
------------------	---

Modulo di	LIBERALIZZAZIONE ED ECONOMIA DELLE TLC
Ore previste:	10

OBIETTIVI DEL CORSO	<p><i>Il modulo si prefigge l'obiettivo di ripercorrere gli eventi storici, da un punto di vista normativo e degli effetti di questi sul mercato, che hanno portato alla liberalizzazione delle TLC, dal monopolio di fine anni '80 al libero mercato dei giorni nostri, con particolare attenzione al Codice delle Comunicazioni Elettroniche del 2003 e delle sue successive modifiche.</i></p> <p><i>Vengono inoltre forniti elementi di valutazione di progetti (business planning) e di analisi di bilanci privatistici con particolare riferimento al mondo delle TLC, analizzando casi ed applicazioni reali.</i></p>
----------------------------	--

PROGRAMMA	<ul style="list-style-type: none">• Dal monopolio alla concorrenza: storia della liberalizzazione delle TLC in Italia<ul style="list-style-type: none">○ Le fasi della liberalizzazione, dalla fine degli anni '80 ad oggi○ Il Codice delle Comunicazioni Elettroniche○ Il listino di interconnessione ed il mercato concorrenziale: evoluzione e regolamentazione• Tecniche di stesura di un business plan<ul style="list-style-type: none">○ Metodologie ed obiettivi○ Principali indicatori (VAN, TIR, PBT, PF)○ Applicazione alle TLC: banda larga ed ultralarga• Analisi di un bilancio privatistico<ul style="list-style-type: none">○ Struttura di un bilancio, stato patrimoniale, conto economico, flussi di cassa○ Indicatori di bilancio○ Applicazione alle TLC: analisi di un bilancio reale di un Operatore○ Confronto tra indicatori, applicazioni a casi reali
------------------	--

Modulo di	LEGISLAZIONE IN MATERIA DI RETI DI TELECOMUNICAZIONE IN TECNOLOGIA 5G
Ore previste:	10

OBIETTIVI DEL CORSO	<p><i>Il modulo si prefigge l'obiettivo di fornire un quadro generale della normativa europea ed italiana in materia di sicurezza delle reti in tecnologia 5G.</i></p>
----------------------------	--

PROGRAMMA	<ul style="list-style-type: none">• Cenni sulle caratteristiche reti in tecnologia 5G• Art. 1-bis del DL 21/2012: Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G
------------------	--



- Raccomandazione (UE) 2019/534 – Sicurezza cyber delle reti 5G
 - Risk assessment europeo sulle reti 5G
 - Toolbox di misure di sicurezza per le reti 5G
- Il ruolo del Centro di Valutazione e Certificazione Nazionale nella sicurezza delle reti 5G
- Comunicazione congiunta del Parlamento Europeo e del Consiglio del 16 dicembre 2020: la strategia di cybersicurezza dell'UE per il decennio digitale

Modulo di

CODICE EUROPEO DELLE COMUNICAZIONI ELETTRONICHE

Ore previste:

10

OBIETTIVI DEL CORSO

Il modulo intende offrire un quadro aggiornato della disciplina delle comunicazioni elettroniche, partendo dall'evoluzione del quadro europeo di riferimento e proseguendo nell'approfondimento dell'attuazione interna delle fonti sovranazionali. L'obiettivo formativo è di far conoscere gli strumenti e gli istituti fondamentali rilevanti nel settore delle comunicazioni digitali, con particolare riferimento alle reti ed ai servizi di comunicazione, alla regolamentazione, nonché alla posizione degli operatori con uno sguardo verso le nuove tecnologie emergenti.

PROGRAMMA

- La disciplina europea delle comunicazioni elettroniche
 - Dal contesto europeo a quello nazionale: l'adeguamento alla disciplina comunitaria e la convergenza
 - La regolamentazione: il ruolo del Ministero e dell'AGCOM
 - Focus: la gestione dello spettro radio e il principio di neutralità tecnologica
- Gli impatti e il valore del settore delle comunicazioni elettroniche per il sistema Paese
 - Il 5G come abilitatore di crescita e competitività delle imprese
 - La gestione e il coinvolgimento degli operatori OTT (over the top) all'interno delle reti e delle infrastrutture
 - La sicurezza delle reti
- Semplificazione dei procedimenti di autorizzazione all'installazione di reti e infrastrutture di comunicazioni elettroniche
 - Le principali iniziative nazionali per favorire lo sviluppo delle infrastrutture fisse e mobili: l'impatto dei decreti semplificazioni e s.m.i
 - Le reti e gli impianti di comunicazione elettronica ad uso pubblico
 - I procedimenti amministrativi per l'installazione e la modifica degli impianti
- Le comunicazioni elettroniche abilitatori di servizi digitale
 - Liberalizzazione e regolamentazione dei mercati
 - Il nuovo quadro normativo europeo per l'era digitale: Proposta di regolamento Gigabit Infrastructure Act, Data Act, DMA, DSA – TUSMAV – Artificial Intelligent Act
 - La convergenza dei servizi (TELCO E MEDIA) verso le tecnologie emergenti (AI, Blockchain, Cloud computing, Computer quantistica)



Modulo di

**L'EVOLUZIONE DEL SISTEMA RADIO TELEVISIVO ITALIANO:
ASPETTI NORMATIVI E TECNICI**

Ore previste

5

**OBIETTIVI DEL
CORSO**

L'obiettivo del modulo è quello di fornire una panoramica dell'attuale stato del sistema radio televisivo italiano, ripercorrendo, sia dal punto di vista normativo che dal punto di vista tecnico, la storia dell'evoluzione del comparto con particolare riferimento ai diversi processi di transizione che, a partire dai primi anni '90, hanno determinato il definitivo passaggio dal sistema analogico a quello digitale, per quanto attiene al comparto televisivo, ed hanno avviato il processo di digitalizzazione del comparto radiofonico.

PROGRAMMA

- Il settore televisivo nazionale e locale fino agli anni '90
 - Stato del sistema fino agli anni '90
 - Inquadramento normativo

- La transizione alla televisione digitale terrestre
 - Motivi e storia della transizione
 - Inquadramento normativo

- L'evoluzione del sistema televisivo con l'avvento del 5G
 - La liberazione della banda a 700 MHz
 - Inquadramento normativo

- Il settore radiofonico nazionale e locale fino agli anni '90
 - Stato del sistema fino agli anni '90
 - Inquadramento normativo

- La radio digitale
 - Stato attuale del sistema
 - Inquadramento normativo



Corso di **PRINCIPI DI INFORMATICA APPLICATA ALLE TLC**

Modulo di **INTRODUZIONE ALLA CYBER SECURITY DEI SISTEMI OT**

Ore previste **20**

OBIETTIVI DEL CORSO

Il modulo si prefigge l'obiettivo di fornire ai discenti una panoramica delle principali problematiche in tema di cyber security con particolare riferimento alle Operational Technologies (OT)

PROGRAMMA

- Cosa è la cyber security
 - Definizioni e obiettivi
 - Motivazioni e Trend
 - Principali modalità di attacco
 - Disamina delle minacce: cyber crime, spionaggio, APT, cyberwar
- Introduzione alle Operational Technologies.
 - Principi di funzionamento, architetture, protocolli e prodotti
 - Peculiarità dei sistemi OT
 - Analisi delle problematiche cyber per sistemi OT ed illustrazione di casi esemplificativi di attacco cyber
- Contromisure
 - Elementi di valutazione del rischio (CVE,CVSS)
 - Principi di cyber security
 - L'utilizzo delle tecniche OSINT
 - Cenni alla direttiva CER

Modulo di **ATTACCHI CRITTOGRAFICI E BLOCKCHAIN**

Ore previste **30**

OBIETTIVI DEL CORSO

*Il modulo ha l'obiettivo di coprire tre macro-argomenti: i) **crittografia applicata**, con specifica attenzione alle modalità di applicazione degli algoritmi crittografici ed agli errori da evitare nell'integrazione della crittografia nei sistemi; ii) **protocolli per la sicurezza delle comunicazioni**, con approfondimento specifico sul protocollo TLS e sui relativi attacchi, ma studiato come esempio concreto di progetto di un "generico" protocollo, e iii) **introduzione alle blockchain**.*

PROGRAMMA

- Motivazioni ed esempi di errori comuni in sicurezza
- Esempio di errore #1: uso errato dell'assunzione di one-time-pad in un contesto di autenticazione mutua con RFID
- Richiami su PAP e CHAP (autenticazione Challenge-Response)
- Esempio di errore #2: problemi dall'uso di CHAP per autenticazione mutua (attacchi di reflection/intertwining) e "soluzione finale"
- Confronto CHAP vs PAP al variare dei modelli di attacco, e considerazioni su sicurezza "relativa" (esempio di errore #3)
- Richiami su protezione delle password mediante hash; perché con CHAP non è possibile farlo; tecnica di mitigazione basata su "salt"; differenze con "salt" integrato nei database delle password



- Ancora sui modelli di attacco: perché non usare SHA-256 nei file di password (cenni a bcrypt)
- Richiami su stream cipher. Definizione di sicurezza semantica (IND-CPA). Il concetto di Initialization Vector
- Esempio di errore #4: il caso WEP: attacco alla confidenzialità a causa di IV completamente sottodimensionato (cenni anche a debolezze RC4 ed attacco Fluhrer-Mantin-Shamir)
- Esempio di errore #4: il caso WEP: attacco all'integrità e problema di linearità del CRC
- Esempio di errore #4: il caso WEP: Autenticazione in WEP e doppio errore: i) attacco all'autenticazione stessa con esempio di impersonation attack, e ii) uso dell'autenticazione WEP per produrre coppie IV->keystream valide ed attaccare cifratura
- Cenni a evoluzione di Wi-Fi security post-WEP
- Introduzione a TLS: handshake e record phases; processo di trasformazione dei dati in trasmissione e discussione
- Richiami su Message Authentication Codes: protezione ad attacchi MITM, protezione ad attacchi SPOOFING, NON protezione a replay attack; concetto di Nonce, le tre forme di nonce (seq, random, timestamp) e discussione di pro e contro per ciascuna categoria
- MAC con Hash: perché il problema NON è banale. Cosa succede con costruzione $H(\text{msg}, \text{segreto})$ (precomputation attack); cosa succede con costruzione $H(\text{segreto}, \text{msg})$ (message expansion attack)
- HMAC: cenni alla costruzione, uso di HMAC
- Ripasso su crittografia a Blocchi: ECB, come rendere ECB semanticamente sicuro. La costruzione CBC
- Il problema della combinazione MAC ed encrypt: le tre possibilità e perché la soluzione MAC and ENC usata in SSH è clamorosamente errata (definizione di sicurezza e sua confutazione con game IND-CPA)
- Richiami su padding TLS
- Risposte del server SSLv3 e TLS1.0 a messaggio errato: decryption_failed vs bad_record_MAC: Padding Oracle Attack. Perché è difficile da mitigare: Canvel side channel 2003
- Parentesi su side channel attack, e cenni ad evoluzioni successive dell'attacco Padding Oracle: Lucky 13, Lucky ms, etc e conclusione con Citazione di Marlinspike (Cryptographer's doom)
- Il problema dell'IV predicibile in CBC: teoria e pratica (BEAST attack, con introduzione al concetto di Chosen Boundary Attack e linearità dell'attacco con dimensione dei token di autenticazione – demo youtube)
- Problemi emergenti con combinazione di compressione e cifratura: CRIME attack (idee di base)
- TLS Handshake: introduzione, obiettivi, richiami su crittografia asimmetrica (RSA key transport e Diffie-Hellman key agreement)
- Il problema dei downgrade attack e dei bid-down attack (con esempi 5G)
- Negoziazione in TLS ed attacco downgrade alla versione. Mitigazione con RSA transport; soluzione definitiva con finished message. Generalizzazione ed applicazione della stessa tecnica difensiva ad altri sistemi
- Gestione delle chiavi in TLS. Extract & Expand: motivazione, esempi, applicazione specifica al caso TLS, PRF e la nuova funzione HKDF (cenni)
- Approfondimento sulla sicurezza di RSA key transport. RSA e Chosen Ciphertext Attack; malleability di RSA
- RSA padding PKCS1v1.5: perché (malleability e CPA), dettagli



- Bleichenbacher Oracle: dove nasce, cosa comporta, vulnerabilità nelle versioni TLS precedenti a 1.0, patch protocollari e relativi limiti
- La saga dell'oracolo di Bleichenbacher dal 1998 al 2019. Perché è veramente difficile mitigare l'attacco. Dettagli sugli attacchi DROWN e ROBOT, e discussione errori di configurazione (es. riuso chiavi) e di implementazione (cenni a protocol fuzzying). Conclusioni (è uno dei tre motivi per cui RSA è stata tolta da TLS1.3)
- Il problema dell'integrità di sessione. Perché non è risolto da HMAC. Soluzione TLS: close-notify
- Renegotiation attack in TLS: quale errore è stato fatto nella standardizzazione, e come è stato sfruttato
- Renegotiation attack in pratica: perché un apparentemente innocuo Plaintext preamble injection attack può invece avere effetti disastrosi in adeguati scenari applicativi. Esempi semplificati ma ispirati all'attacco di Kurmus a twitter
- Cenni a TLSv1.3, con particolare approfondimento sul concetto di Perfect Forward Secrecy e la sua importanza attuale. Perché solo Ephemeral DH permette PFS. PFS con pre-shared key: come si ottiene. Cenni a PFS in applicazioni di messaggistica (signal double ratchet).
- Altri asset di TLS1.3 (cenni veloci): 3way handshake, 0-rtt, restrizione ai soli cipher AEAD, etc.
- Mass surveillance in TLS e problematiche emergenti con la PKI (problema dei certificati Fake e scenari di attacco)
- La soluzione Certificate Transparency / Extended Validation
- Dettagli tecnici su Merkle Tree / Cron Tree ed applicazione a Certificate Transparency
- Introduzione alle Blockchain. Definizione, giustificazione, perché l'organizzazione a blocchi di Certificate Transparency non è una blockchain
- Differenze tra permissionless[DD1] vs permissioned
- Architettura e struttura dati di una blockchain; come gestire l'identità per utenti anonimi: self-certifying identities
- Consenso: concetto generale, il caso permissioned; perché è difficile nel caso permissionless, consenso implicito nella soluzione bitcoin. Il problema degli attacchi sibilla e cenni a proof-of-work e proof-of-stake; il problema del 51%: attacchi offspring ed implicazioni geo-politiche
- Scripting nelle blockchain: cenni

Modulo di **SICUREZZA INFORMATICA E PREVENZIONE DEGLI ATTACCHI**

Ore previste: **10**

OBIETTIVI DEL CORSO

Il modulo si prefigge l'obiettivo di fornire elementi di base di sicurezza informatica al fine di aumentare la consapevolezza dei principali rischi e migliorare la conoscenza delle relative contromisure da adottare in termini tecnici e comportamentali. Vengono descritti i principali vettori di attacco, tra i quali viene dato ampio spazio al phishing ed alle relative metodologie di social engineering, lo sfruttamento di vulnerabilità e l'utilizzo di malware, fornendo parallelamente tutti gli elementi tecnici e, soprattutto, comportamentali, per evitare di diventare vittime di crimini informatici mettendo in pericolo i propri dati, sia come cittadini che come lavoratori all'interno di una organizzazione.

PROGRAMMA

- Introduzione: definizione e panoramica dei rischi e degli attacchi informatici
- Phishing



- Rischi e contromisure
- Social engineering e spear phishing
- Tecniche di protezione: analisi dell'header, SPF, DKIM, DMARC
- Malware
 - Tecniche di attacco attraverso malware: classificazione del malware
 - Analisi del malware: statica e dinamica, analisi di casi reali
 - Botnet: struttura, analisi e tecniche di attacco; attacchi DDoS
- Vulnerabilità
 - Definizioni, CVE e CVSS
 - SQL Injection, tecniche di attacco e contromisure
 - Data breach: rischi e mitigazione
 - XSS (Cross Site Scripting): tecniche di attacco e contromisure
- Crittografia e protezione dei dati
 - Cenni di crittografia simmetrica ed asimmetrica
 - Funzioni hash
 - Cenni di steganografia

Modulo di **SISTEMI BIOMETRICI**

Ore previste: **10**

OBIETTIVI DEL CORSO

Il modulo si propone l'obiettivo di fornire gli strumenti per comprendere ed analizzare i sistemi biometrici che utilizzino sia una sola caratteristica biometrica (sistemi uni-modal) che più caratteristiche biometriche (sistemi multi-modal).

PROGRAMMA

- **Fondamenti di Biometria:** Identità e biometria. Introduzione ai sistemi biometrici. Applicazioni
- **Identificatori biometrici morfologici:** impronte digitali, volti (2D e 3D), geometria della mano, palmo della mano, strutture venose, iride, termogrammi, etc.) e comportamentali (firma, voce, modalità di digitazione, andatura, movimento delle labbra, etc.)
- **Verifica e valutazione delle prestazioni del sistema:** FAR, FRR. FTE, FTA, curve ROC, DET, CMC, usabilità, scalabilità
- **Sistemi biometrici multimodali**

Modulo di **HARDWARE SECURITY**

Ore previste: **20**

OBIETTIVI DEL CORSO

L'obiettivo del modulo è di introdurre le problematiche di cybersicurezza collegate all'hardware sia per quanto riguarda l'inserimento di "Hardware Trojan" sia per quanto riguarda le vulnerabilità relative ai Side Channel Attack. Vengono poi introdotte e discusse le possibili contromisure.

PROGRAMMA

- Introduction and background notions
 - Introduction to Hardware Security & Trust
 - Introduction to Cryptography
 - Basics of VLSI Design and Test and Reliability
- Trust Issues



-
- Hardware Trojans
 - Trojan Modeling
 - HWT Examples
 - HWT in FPGA Designs
 - Activation
 - Payload
 - Location
 - Trojans Taxonomy
 - Trust Benchmarks
 - Vulnerability Issues
 - Side Channel Attacks
 - Taxonomy of SCA
 - Simple Power Analysis
 - Differential Power Analysis
 - Transient execution attacks
 - Fault Attacks
 - Manufacturing test issues
 - Covert channels
 - Test oriented attacks
 - Countermeasures
 - Security assets and model attacks
 - Countermeasures against trust Issues
 - IP level (pre silicon) validation
 - Formal verification and coverage
 - IC level (post-silicon) validation
 - Taxonomy of HWT detection
 - Design for HW Trust
 - Countermeasures against vulnerability Issues
 - Anti DPA countermeasures
 - Anti EMA countermeasures
 - Anti-Timing attack
 - Hardware security primitives
 - Physically Unclonable Functions
 - PUF classification
 - PUF quality
 - Common PUF architectures
 - PUF applications
 - True Random Number Generators
 - TRNG Quality properties



Modulo di **MODELLI DECISIONALI E INTELLIGENZA ARTIFICIALE**

Ore previste: **20**

OBIETTIVI DEL CORSO

Lo scopo del modulo è quello di introdurre gli studenti all'uso di strumenti analitici per affrontare problemi decisionali. Gli strumenti includono la definizione di modelli matematici prescrittivi, modelli descrittivi di simulazione e di intelligenza artificiale e l'uso di algoritmi per individuare una buona soluzione del problema in esame. Sarà data anche enfasi all'applicazione di tali strumenti nel settore TLC.

PROGRAMMA

- I. Introduzione alla decision analytics
 - Decision analytics: definizione e differenza tra metodi descrittivi, predittivi e prescrittivi
 - Vantaggi dell'utilizzo delle tecniche di decision analytics nell'ambito delle telecomunicazioni
 - Esposizione di casi applicativi rilevanti nel settore TLC
- II. Metodologie di decision analytics
 - II.a Machine learning e reti neurali
 - Machine learning: definizioni; paradigmi di apprendimento supervisionato e non supervisionato
 - Modelli di clustering
 - Modelli di classificazione: le reti neurali artificiali, alberi e foreste
 - II.b Modellistica per la prescriptive analytics
 - Definizione del problema e raccolta dei dati
 - Costruzione e validazione del modello
 - Utilizzo dei modelli per la pianificazione e l'ottimizzazione delle decisioni
 - Modelli prescrittivi e ottimizzazione: ruolo, caratteristiche, classificazione e metodologie principali
 - II.c Metodi e modelli di simulazione
 - Classificazione delle tecniche di simulazione
 - Modelli di sistemi di servizio e simulazione
 - Simulazione ad eventi discreti: caratteristiche ed applicazioni
- III. Applicazioni di metodi e modelli di decision analytics nel settore delle telecomunicazioni e casi di studio di processi decisionali in ambito strategico, tattico e operativo:
 - Progetto e pianificazione di reti e di capacità
 - Gestione delle risorse, del traffico e dell'esperienza del cliente
 - Analisi e miglioramento di processi aziendali



Corso di **SERVIZI, RETI E TERMINALI DI TLC**

Modulo di **SCIENZE SOCIALI, PIATTAFORME E INTERFACCE**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo si prefigge l'obiettivo di proporre il contributo delle scienze sociali (e, in particolare, sociologia della comunicazione e internet studies) all'analisi e all'interpretazione dei fenomeni legati all'utilizzo delle piattaforme e degli ambienti digitali.

PROGRAMMA

- Rapporto tecnologia/cultura/società
 - Mutual shaping tecnologia/società
- Gli algoritmi dei social media e di Google – dal punto di vista dello scienziato sociale
 - Immaginari algoritmici
- I processi di convergenza
- I modelli: network society e platform society
- Struttura e dinamiche dei network (dal punto di vista dello scienziato sociale)
- Social media e social network site
- Gli utenti dei sistemi digitali
 - “Nascita degli utenti” (e della HCI)
 - Evoluzione della riflessione sugli utenti
 - Un focus: il concetto di “utente modello”
 - Anziani e ICT: tra ageism e “unexpected users”
- Interfacce
 - User experience
 - Human centered design

Modulo di **VALUTAZIONE DELLA QUALITÀ E USABILITÀ DEI SITI WEB**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo didattico è strutturato per trasferire conoscenze e competenze specialistiche sugli aspetti della multimedialità e della sua convergenza nelle reti e nella tv digitale, nonché sulle caratteristiche dei servizi multimediali e sui metodi di verifica della loro qualità. La didattica comprende e si completa poi, con una parte dedicata ai servizi digitali nel web, sui requisiti di qualità che devono avere in termini di contenuti, accessibilità, usabilità e sui metodi e gli strumenti per valutarli. La sezione teorica per l'acquisizione delle conoscenze scientifiche e normative è integrata ed arricchita con una serie di esperienze pratiche, svolte grazie all'ausilio dei laboratori della DGTCSI-ISCTI.



PROGRAMMA	<ul style="list-style-type: none">• Raccomandazioni e Specifiche sulla QoS o Organismi di standardizzazione<ul style="list-style-type: none">o Normative sulla QoS e QoE della reteo Qualità percepita dall'utente• Il progetto Misurainternet<ul style="list-style-type: none">o La certificazione dei sistemi di misurao Il test Plant utilizzato per la certificazione• Usabilità dei siti web<ul style="list-style-type: none">o L'usabilitào Il protocollo eGLUo I test di usabilità con utenti disabilio I progetti di ricerca di ISCTI sull'usabilità• Attività di laboratorio o Test di usabilità con protocollo eGLU
------------------	---

Modulo di	ACCESSIBILITÀ DEL WEB
Ore previste:	20

OBIETTIVI DEL CORSO	<i>Il modulo è strutturato per trasferire conoscenze e competenze specialistiche sugli aspetti legati ai requisiti di qualità e all'accessibilità dei contenuti e dei servizi digitali nel web, con particolare riguardo ai metodi e agli strumenti per valutarli. La sezione teorica per l'acquisizione delle conoscenze scientifiche e normative è integrata ed arricchita con una serie di esperienze pratiche, svolte grazie all'ausilio dei laboratori della DGTCSI-ISCTI.</i>
----------------------------	---

PROGRAMMA	<ul style="list-style-type: none">• Introduzione all'accessibilità<ul style="list-style-type: none">o Concetti generalio Disabilità e tecnologie assistiveo Dislessia e buone pratiche di progettazione• Normativa e standard di riferimento<ul style="list-style-type: none">o EN 301 549 e linee guida W3C WCAG 2.1o Legge n. 4/2004 e s.m.i.• Introduzione alle tecnologie del web<ul style="list-style-type: none">o HTMLo CSS• Requisiti tecnici<ul style="list-style-type: none">o Criteri di successoo Tecniche di accessibilità• Verifiche di accessibilità<ul style="list-style-type: none">o Metodologiao Strumenti di valutazione• Attività e pratiche di laboratorio<ul style="list-style-type: none">o Esecuzione delle verifiche di accessibilità in esercitazione di gruppoo Analisi dei risultati e redazione del rapporto di prova
------------------	---



Corso di **TECNOLOGIE ELETTRONICHE E TECNICHE CIRCUITALI**

Modulo di **SISTEMI DI COMUNICAZIONE IN FIBRA OTTICA**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo si propone l'obiettivo di fornire le conoscenze principali relative ai sistemi di comunicazione in fibra ottica. Obiettivi del corso sono l'analisi delle prestazioni di tali sistemi sia in configurazione punto-punto sia nell'ambito delle reti ottiche (rete di trasporto e rete d'accesso). Sono forniti gli strumenti di base per la progettazione di tali sistemi.

PROGRAMMA

- **FIBRE OTTICHE**
 - Fibre ottiche: analisi mediante l'ottica geometrica; fibre ottiche multimodali, apertura numerica, dispersione modale
 - Fibre ottiche singolo-modo: analisi mediante l'ottica fisica; modo fondamentale, cut-off, attenuazione
 - Dispersione cromatica: dispersione del materiale, dispersione di guida
 - Tipi di fibra ottica singolo-modo: SM (G.652), DS (G.653), NZDF (G.655)
 - Propagazione in fibra ottica in regime lineare
 - Fenomeni non-lineari: effetto Kerr (SPM, FWM, XPM)
 - Propagazione in fibra ottica in regime non-lineare (solitoni)
 - Fenomeni di scattering in fibra ottica: effetto Brillouin, effetto Raman
- **SORGENTI OTTICHE**
 - Interazione luce-materia
 - Laser a semiconduttore
- **COMPONENTI IN OTTICA INTEGRATA**
 - Effetto elettro-ottico lineare (effetto Pockels)
 - Modulatori elettro-ottici di ampiezza e di fase (LiNbO₃)
- **RICEVITORI OTTICI**
 - Fotodiodi: PIN, APD, efficienza quantica, responsività, rumore di rivelazione (shot-noise)
 - Struttura del ricevitore ottico a rivelazione diretta (DD): amplificatore di front-end (amplificatore a transimpedenza, amplificatore ad alta impedenza)
 - Sensibilità del ricevitore. Limite quantico della rivelazione ottica
 - Prestazioni del ricevitore ottico: rumore termico, rapporto segnale-rumore (SNR), probabilità d'errore di bit (BER)



Modulo di **COMPETENZE DI OPTOELETTRONICA**

Ore previste: **20**

OBIETTIVI DEL CORSO

Il modulo si prefigge l'obiettivo di fornire una panoramica completa dei dispositivi optoelettronici alla base dei sistemi di comunicazione ottica.

PROGRAMMA

- Introduzione alle reti ottiche
 - Dispositivi e funzioni 1R, 2R 3R
 - Proprietà ed utilizzo delle fibre ottiche
- Proprietà dei semiconduttori
 - L'archetipo dei dispositivi optoelettronici a stato solido: la giunzione p-n
 - Classificazione principali dispositivi optoelettronici
 - Concetti di base sui materiali semiconduttori. Fondamenti del trasporto di carica. Proprietà ottiche dei semiconduttori. Cenni su giunzioni p-n e diodi p-i-n. Eterostrutture: proprietà di base ed applicazioni
- Dispositivi optoelettronici fondamentali
 - Fotorivelatori
 - Assorbimento intrinseco ed efficienza quantica. Fotorivelatori a diodo p-i-n. Fotorivelatori a valanga (APD). Fotorivelatori ad eterogiunzione. Sistemi ed applicazioni: Free Space Optics, Visible Light Communications
- Dispositivi optoelettronici fondamentali
 - LED
 - LASER multimodali (Fabry-Perot)
 - Assorbimento, emissione spontanea ed emissione stimolata. Guadagno ottico. Emissione spontanea. Spettro della radiazione di ricombinazione. Efficienza quantica. Modulazione della radiazione ottica. Principi di funzionamento di LED. Applicazioni dei LED
 - LASER: Emissione stimolata. Principi dell'azione laser. Proprietà della radiazione laser. Guadagno ottico in semiconduttori. Rate equations per Laser a semiconduttori
- Dispositivi optoelettronici avanzati
 - Amplificatori ottici (SOA, EDFA, Raman)
 - Sistemi ottici per l'elaborazione ottica dell'informazione
 - Case study (esercitazione di laboratorio): il caso della conversione di lunghezza d'onda per i sistemi WDM mediante effetti ottici non lineari negli amplificatori a semiconduttore
 - Esempi di sistemi di comunicazione ottica. Sistemi WDM, architetture di routing ottico, conversione di lunghezza d'onda mediante dispositivi ottici non lineari, esercitazione di laboratorio su amplificazione ottica, modulazione, conversione di lunghezza d'onda mediante XGM
- Dispositivi optoelettronici avanzati
 - LASER monocromatici avanzati (DFB, DBR)
 - Dispositivi per la modulazione esterna (Niobato di Litio, modulatori ad elettroassorbimento)
 - Tipi di modulatori, architetture e principi di funzionamento



Corso di UTILIZZAZIONE E ALLOCAZIONE DELLO SPETTRO RADIO

Modulo di PIANIFICAZIONE E GESTIONE DELLO SPETTRO RADIO

Ore previste: 20

OBIETTIVI DEL CORSO

Il modulo si propone l'obiettivo di fornire i concetti base della pianificazione e della gestione dello spettro radio, mettendo in risalto la necessità di stabilire regole adottate a livello mondiale. La risorsa naturale «spettro radio» si propaga in spazi non limitati che vanno oltre i confini nazionali, pertanto è necessario armonizzare le regole attraverso Organismi internazionali di regolamentazione.

Nella prima parte, il modulo illustra i principi di carattere generale della risorsa spettro radio dopodiché descrive la struttura degli Organismi internazionali, il metodo di lavoro e gli Atti Normativi. Poi si cala nella descrizione degli Organismi italiani e nella trattazione dettagliata delle principali norme quali il Regolamento mondiale delle radiocomunicazioni dell'UIT, il PNRF (Piano Nazionale di Ripartizione delle Frequenze) ed il Codice delle Comunicazioni Elettroniche.

Nella seconda parte, il modulo descrive i principali processi ed attività utilizzati nella gestione dello spettro radio ed illustra l'evoluzione degli scenari di radiocomunicazione e delle tecnologie di trasmissione radio fino alla tecnologia 5G.

PROGRAMMA

- Introduzione all'attività di pianificazione e gestione dello spettro radioelettrico
 - Caratteristiche dello spettro radio, risorsa scarsa
 - Necessità di coordinamento e regole armonizzate a livello mondiale
 - Attribuzione delle frequenze radio, servizi radio e stazioni radio
 - Servizi primari e secondari e regole del coordinamento
 - Ruolo dell'Organismo nazionale
- Unione Internazionale delle Telecomunicazioni (UIT)
 - Compiti e struttura dell'UIT
 - Il Regolamento delle Radiocomunicazioni
 - Conferenze Mondiali delle Radiocomunicazioni
- Organismi europei di regolamentazione. Compiti, obiettivi, struttura e attività
 - CEPT
 - Unione Europea
 - ETSI
- Organismi e normativa nazionale.
 - Il Ministero delle Imprese e del Made in Italy (MIMIT)
 - Il Ministero della Difesa
 - L'Autorità per le Garanzie nelle comunicazioni
 - Piano Nazionale di Ripartizione delle Frequenze
 - Piani di Assegnazione e di Allocazione delle frequenze
- Il Codice delle comunicazioni elettroniche
 - Semplificazioni apportate dal codice (neutralità dei servizi e delle tecnologie, vendita ed affitto secondario delle frequenze, ...)
 - Autorizzazione generale per l'esercizio di reti e servizi di comunicazione elettronica: SCIA e diritti d'uso delle frequenze
 - WISP (Wireless Internet Service Provider)
 - Uso collettivo dello spettro radio e Short Range Devices (SRD)
- Nuovi scenari nella gestione dello spettro radio
 - Convergenza dei servizi radio, delle tecnologie e delle infrastrutture di rete
 - Reti di accesso radio - WiFi, WiMax, WLL26/28 (Wireless Local Loop, FWA)



- Tecniche di condivisione dello spettro radio, Tecnologie cognitive e Licenced Shared Access (LSA)
- Sperimentazione di rete LSA in banda 2300-2400 MHz - MISE Roma EUR
- Pianificazione dello spettro radio per le reti IMT2020 e 5G ed evoluzione delle reti mobili
 - UIT-R - Identificazione delle bande IMT
 - Introduzione, obiettivi e scenari d'uso delle reti in tecnologia 5G
 - Evoluzione delle reti mobili (slicing della rete, reti eterogenee)
 - Piano d'azione e roadmap dell'UE e della CEPT
 - Bande di frequenze pioniere (3400-3800 MHz 24,25-26,5 GHz)
 - Introduzione del 5G in Italia, sperimentazione e bando di gara del 2018

Modulo di

DIGITAL SINGLE MARKET: REGOLAMENTAZIONE E STANDARDIZZAZIONE

Ore previste:

10

OBIETTIVI DEL CORSO

Il modulo si prefigge di fornire la chiave di lettura per decodificare, dal punto di vista industriale ed economico, la portata del Mercato Unico Digitale (in particolare dei prodotti radio) nel mercato interno, attraverso una analisi delle disposizioni regolamentari, della standardizzazione, dell'NLF e delle iniziative sulla cyber security.

PROGRAMMA

MERCATO UNICO

- ONE SINGLE MARKET
 - Timeline del processo di apertura del mercato
 - Digital Single Market and e-Commerce
 - Prospettive 2024, 2030, 2050
 - Mercato B2C - B2B - C2C - B2G, (Business – Commercial – Government)
 - e-procurement, e-signature
 - Cenni sul Regolamento EIDAS su trust services
 - Common standards for Digital Single Market
- GOODS MARKET
 - Building blocks of the Single Market
 - New Legislative Framework: Regolamenti e decisioni costituenti l'attuale quadro regolamentare e le prospettive future (Reg. 765/2008/CE e 2019/1020 UE, Dec. 768/2008/CE, Reg. 764/2008/CE e altri documenti di indirizzo). In particolare: migliorare le regole per la vigilanza del mercato, aumentare la qualità (e la fiducia) della valutazione della conformità dei prodotti, istituire un quadro giuridico comune che comprende la sicurezza informatica (proposta di Regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali)
 - Notified Body
 - Conformity Assessment Body
 - Conformity Assessment Procedure
 - Market surveillance
 - Esempio di direttiva generica (EMC)
- RADIO EQUIPMENT MARKET
- DIRETTIVA 2014/53/UE sulle "apparecchiature radio"



- Scopo
- Requisiti essenziali, CAB, CAP, NB
- Effective Vs Efficient
- Prodotti “faster than regulation”
- Study cases: “La SAR nei telefonini”, Il caso “Cayla”, Il caso degli “zainetti”
- GLI STANDARDS NEL CONTESTO REGOLAMENTARE EUROPEO E MONDIALE
 - European Standard
 - Study case “James Elliott vs Irish Asphalt Limited”
 - International standard
 - Regolamento 1025/2012 e varie modifiche
 - ESO (European Standardisation Organisations) SDO (Standard Developing Organizations)
 - Le azioni intraprese per la protezione del mercato interno da holding di soggetti terzi

Modulo di

**SISTEMI SATELLITARI, INGEGNERIA DELLO SPETTRO
ELETTROMAGNETICO E REGOLAMENTAZIONE INTERNAZIONALE**

Ore previste:

10

OBIETTIVI DEL CORSO

Brevi cenni sulle principali nozioni di dinamica orbitale, delle tecniche di telecomunicazione e trasmissione delle onde elettromagnetiche nello spazio, per comprendere i principi necessari a garantire un'equa distribuzione, fra i numerosi operatori, delle risorse disponibili in termini di posizioni orbitali e spettro elettromagnetico. Il corso include alcuni elementi teorici per l'apprendimento delle tecniche necessarie alla valutazione delle interferenze fra costellazioni geostazionarie e non geostazionarie anche attraverso l'utilizzo dei principali strumenti software.

PROGRAMMA

- I sistemi satellitari (4 ore)
 - Cenni di dinamica orbitale
 - I principi delle Comunicazioni Satellitari
 - Stazioni di terra e collegamenti satellitari
 - Reti e sistemi di comunicazione
- Interferenze e Regolamentazione (4 ore)
 - Regolamentazione Internazionale e regionale
 - I concetti base dell'ingegneria dello spettro elettromagnetico
 - I modelli di propagazione delle onde elettromagnetiche
 - Il calcolo delle interferenze
- Gli strumenti software (2 ore)
 - Strumenti software per le analisi delle interferenze
 - Il software dell'ITU
 - Software disponibili sul mercato



Modulo di **CAMPI ELETTROMAGNETICI – NORMATIVA E STRUMENTAZIONE**

Ore previste: **10**

OBIETTIVI DEL CORSO

Il modulo si propone l'obiettivo di fornire un livello di conoscenza approfondita ed integrale dei campi elettromagnetici sia in alta frequenza sia in bassa frequenza, della normativa nazionale ed internazionale ad essi applicabile, dei principi di funzionamento della strumentazione di misura (con possibilità di eventuale laboratorio di 5 ore aggiuntive per attività di misurazione delle sorgenti in alta frequenza presso i laboratori del Ministero delle Imprese e del Made in Italy mediante analizzatori di spettro e antenne in dotazione presso i laboratori stessi).

PROGRAMMA

- Presentazione del corso
- ICNIRP – Linee Guida del 1998
- D.M. 10 settembre 1998 n.381
- Raccomandazione 519/CEE/1999
- Legge quadro 22 febbraio 2001 n. 36
- DPCM 8 luglio 2003 – ELF
- Strumentazione di misura ELF
- Proprietà dei campi ELF
- Pressioni sul territorio nazionale di sorgenti di campi elettromagnetici
- SAR – tasso di assorbimento specifico e classificazione IARC
- Le agenzie regionali sul territorio: attività e compiti
- Statistiche e analisi dei dati aggiornati
- Sistema agenziale per il 5G
- Saturazione dei siti
- Campi da elettrodotti e da cabine e sottostazioni elettriche
- DPCM 8 luglio 2003 RF
- Decreto-legge 18 ottobre 2012 n.179
- Sistema Agenziale – ISPRA e ARPA
- DM 2 dicembre 2014 – Linee guida ISPRA/ARPA
- Linee guida ICNIRP 2020
- Centraline di monitoraggio
- Legge 111/2011 articolo 35
- Direttiva UE 2018/1972
- Nuovo Regolamento Europeo 30 giugno 2020
- Decreto legislativo 207/2021
- Presentazione delle attività di misura
- Proprietà dei campi: campo vicino e campo lontano, etc.
- Caratteristiche generali della strumentazione
- Strumentazione a banda larga
- Strumentazione a banda stretta
- Analizzatore di spettro e tecniche di misura
- Norma CEI 211-7 e misurazione da impianti AM, FM, DVBT, GSM, LTE, UMTS e 5G
- Esempio numerico di misurazione in banda stretta
- Software di simulazione dei CEM
- Tecniche di estrapolazione
- Tecniche di riduzione a conformità
- Incertezza di misura
- Taratura della strumentazione

