**Allegato 1 al Regolamento dei Corsi di Master, di Perfezionamento e di Aggiornamento**

PARTE I - INFORMAZIONI GENERALI

|  |  |
| --- | --- |
| **Tipologia di corso** | Master di secondo Livello |
| **Titolo del corso** | La cybersecurity per la protezione dei sistemi di controllo nell’industria 4.0 e nelle infrastrutture critiche |
| **Il corso è** | Nuova istituzione |
| **Denominazione nell’a.a. precedente** |  |
| **Dipartimento proponente** | Dipartimento Ingegneria |
| **Corso interdipartimentale** | NO |
| **Corso in collaborazione con enti privati e/o pubblici** | Accenture, Ordine Ingegneri Roma, Competence Center Cyber 4.0., AIIC, Siemens Automation, Beckoff Automation, Shnaider, General Electrics, Rockwell Automation |
| **Corso in collaborazione con università italiane e/o straniere** | NO |
| **Rilascio titolo congiunto** | NO |
| **Durata prevista** | 31 gennaio 2021 - 27 settembre 2021  La prova finale si terrà entro dicembre 2021 |
| **Date presunte di inizio e fine corso** | 31 gennaio 2021 - 27 settembre 2021 |
| **Sede del corso** | Dipartimento di Ingegneria dell’Università degli Studi Roma Tre, Via Vito Volterra 62, Roma |
| **Segreteria del corso** | Dipartimento di Ingegneria dell’Università degli Studi Roma Tre, Via Vito Volterra 62, Roma.  Segreteria didattica: Silvia Mandolini 0657333397.  Segreteria amministrativa: Simona Catallo: 0657333219. |

Direttore del Corso

|  |  |  |  |
| --- | --- | --- | --- |
| **Cognome** | **Nome** | **Dipartimento** | **Qualifica** |
| Panzieri | Stefano | Ingegneria-Università  degli Studi Roma Tre | Professore Ordinario |

Consiglio del Corso

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Cognome** | **Nome** | **Dipartimento/Ente** | **Qualifica** |
| **1** | **Il Direttore quale Presidente**  **Prof. Panzieri** | **Stefano** | Ingegneria-Università degli Studi Roma Tre | Professore Ordinario |
| **2** | Rocco | Paola | Ordine degli Ingegneri Roma | Presidente Commissione Sicurezza Informatica |
| **3** | Tieghi | Enzo | Servitecno S.r.l. | CEO |
| **4** | Neri | Alessandro | Ingegneria-Università  degli Studi Roma Tre | Prof. Ordinario |
| **5** | Di Battista | Giuseppe | Ingegneria-Università degli Studi Roma Tre | Prof. Ordinario |
| **6** | Pascucci | Federica | Ingegneria-Università degli Studi Roma Tre | Ricercatore |
| **7** | Molinaro | Marco | Accenture | Managing Director |
| **8** | Maurizio | Pizzonia | Ingegneria-Università degli Studi Roma Tre | Prof. Ordinario |
| **9** | Foglietta | Chiara | Ingegneria-Università degli Studi Roma Tre | RTD-A |

Docenti dell’Ateneo impegnati nell’attività didattica \*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Cognome** | **Nome** | **Dipartimento** | **Qualifica** | **Numero di CFU impartiti** |
| **1** | Panzieri | Stefano | Ingegneria-Università  degli Studi Roma Tre | Professore Ordinario | 2,5 |
| **2** | Pizzonia | Maurizio | Ingegneria-Università  degli Studi Roma Tre | Ricercatore | 2 |
| **3** | Neri | Alessandro | Ingegneria-Università  degli Studi Roma Tre | Professore  ordinario | 2 |
| **4** | Pascucci | Federica | Ingegneria-Università  degli Studi Roma Tre | Ricercatore | 1 |
| **5** | Foglietta | Chiara | Ingegneria-Università  degli Studi Roma Tre | Ricercatore | 5 |
| **6** | Riccardo | Torlone | Ingegneria-Università  degli Studi Roma Tre | Ordinario | 1 |

*\*Sono indicati i docenti dell’Ateneo impegnati nell’attività didattica della prossima edizione del corso.*

Esperti impegnati nell’attività didattica \*\*

I docenti impegnati nella didattica, oltre a quelli interni già elencati, saranno indicati in seguito di procedure comparative appositamente svolte.

PARTE II - REGOLAMENTO DIDATTICO ORGANIZZATIVO

|  |  |
| --- | --- |
| **Analisi del fabbisogno formativo** | Con il diffondersi di internet in ambito industriale ogni dispositivo connesso alla rete, sensore, server o periferica connessa, è un potenziale punto di attacco.  L’approccio per la protezione di tali infrastrutture in ambito Operational Technology è complesso e non può essere lo stesso adottato per i sistemi IT. La sicurezza in ambito OT infatti si concentra sulla difesa di sicurezza fisica (safety), affidabilità (reliability) e produttività (productivity), parametri evidentemente diversi da quelli della sicurezza informatica.  È necessario quindi formare esperti che conoscano tali infrastrutture e che ne possano progettare la sicurezza. |
| **Il Corso di Studio in breve** | Il Master, si propone l’obiettivo di una formazione specialistica post lauream in materia di protezione dei sistemi SCADA, PLC e su Iot. L’iter formativo prevede l’acquisizione di elevate competenze teoriche e pratiche in ambito network security, apparati per il monitoraggio delle reti industriali, treat modeling, penetration test, physical security, analisi e gestione del rischio, cyber security management system ISA99**/IEC 62443.** |
| **Obiettivi formativi specifici del Corso** | Il Master forma la figura di un esperto nella progettazione e gestione dei sistemi preposti alla tutela della sicurezza e alla protezione del patrimonio informativo e architetturale dei sistemi di controllo industriale e per le infrastrutture critiche.  Il corso sarà articolato in sei moduli che formano un percorso completo e strutturato per una figura in grado di muoversi nel settore della Cybersecurity dei sistemi di controllo dalla analisi delle vulnerabilità, alla valutazione del rischio, fino all’individuazione delle contromisure più adatte (IoT/Scada Cybersecurity and Risk Assessment Specialist.).  Saranno possibili anche tre percorsi più brevi per formare delle figure maggiormente settoriali:  Percorso 1 “Sistemi di Automazione Industriale” che forma un tecnico per la programmazione di base di sistemi che fanno uso di controllori industriali (PLC, SCADA).  Percorso 2 “Risk management Specialist per l’Automazione” che consente di formare professioni esperti di tecniche di Risk Assessment specifiche per i sistemi di controllo industriale.  Percorso 3 “Cyber-security expert per l’Automazione” che consente di formare professioni esperti di Disegno progettazione di soluzioni di sicurezza specifiche per i sistemi di controllo industriale. |
| **Sbocchi occupazionali** | Tutte le aziende, dalle PMI alle industrie manufatturiere più grandi fino allle utility che fanno uso di controllori industriali, sistemi IoT e sistemi SCADA per la produzione o distribuzione di beni ed energia. Tutte le società di consulenza che lavorano con le suddette aziende su problematiche di cybersecurity. Tutte le aziende di progettazione e integrazione di sistemi di controllo che vogliono inserire nella loro offerta anche apparati che garantiscano sicurezza informatica. |
| **Capacità di apprendimento** | Attraverso le prove intermedie, previste alla fine di ogni modulo, e mediante la prova finale, consistente nella discussione dell’elaborato di ciascun candidato, sarà verificato il conseguimento degli obiettivi formativi, come sopra specificati.  I risultati di apprendimento attesi consistono, pertanto, nella puntuale verifica dell’acquisizione delle competenze e delle conoscenze indicate come idonee al perseguimento degli sbocchi professionali indicati al punto precedente. |
| **Conoscenza e comprensione** | Alla fine del Master, gli iscritti avranno acquisito competenze specialistiche di elevato livello nell’ambito della sicurezza dei sistemi di controllo industriale e per le infrastrutture.  Saranno in grado di avere piena consapevolezza delle architetture dei sistemi ICS, della normativa nazionale e internazionale sulla cybersecurity applicabile, delle metodologie di analisi, rilevazione e gestione delle minacce informatiche al mondo IIOT. |
| **Capacità di applicare conoscenza e comprensione** | Le competenze teoriche e pratiche acquisite durante il Master permetteranno allo studente di padroneggiare la complessa materia della sicurezza applicata al mondo dei sistemi di controllo industriale e di svolgere attività professionali in tale campo. |
| **Riconoscimento delle competenze pregresse** | Per gli studenti che hanno frequentato e superato il corso di Reti e Sistemi per l’Automazione del Dipartimento di Ingegneria di Roma Tre o altro corso equivalente è riconosciuta l’abbreviazione del corso di Master per quanto riguarda il Modulo 1. |
| **Prove intermedie e finali** | Prove intermedie  Le prove intermedie, collocate al termine dei singoli moduli  didattici, consistono in esercitazioni su casi pratici e/o simulazioni e test di verifica.  Prova finale  La prova consiste nella discussione di un elaborato scritto sui risultati di una field research, assegnata nell’ambito degli  insegnamenti e dei moduli, da depositare almeno venti giorni prima della prova stessa al termine del Corso. |
| **Requisiti per l’ammissione** | Laurea magistrale, specialistica o titolo di studio equipollente in Ingegneria, Fisica, Matematica. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell’interessato.  Per la sola partecipazione ai Moduli 2, 4 e 5 è prevista l’estensione anche alla Laurea magistrale, specialistica o titolo di studio equipollente in Giurisprudenza ed Economia. |
| **Numero minimo e massimo di ammessi** | *- Il n. minimo non può comunque essere inferiore a 12 e il massimo superiore a 25 -* |
| **Criteri di selezione** | *Verrà valutato il Curriculum Vitae e una lettera di motivazione da allegare. Verranno svolti eventualmente colloqui individuali per identificare i candidati migliori in base a criteri che includono: preparazione di base, propensione allo studio, motivazione personale.* |
| **Scadenza domande di ammissione** | Le domande di ammissione scadranno il 31 dicembre 2020. |
| **Modalità didattica** | *Il corso prevede una didattica convenzionale in aula e laboratorio. In alcuni casi le lezioni teoriche potranno essere integrate da videolezioni preregistrate. In caso di situazioni emergenziali è previsto che la didattica possa essere erogata anche con l’aiuto di piattaforme informatiche con preferenza di Microsoft Teams. In ogni caso la piattaforma Teams sarà utilizzata per la distribuzione del materiale didattico dei vari moduli.* |
| **Lingua di insegnamento** | *La lingua di insegnamento è l’italiano salvo la possibilità che possa essere utilizzato l’inglese nel caso di seminari di personalità di spicco .* |
| **Informazioni utili agli studenti** | *Il corso prevede la presenza di uditori nella quantità massima di 10 e l’iscrizione ai singoli moduli/percorsi fatto salvo il numero massimo di presenze quantificate in 35 per i moduli teorici e 25 per quelli pratici.*  Nell’ambito del piano didattico del Master è possibile: 1) l’iscrizione all’intero Corso di Master; 2) l’iscrizione a singoli Percorsi ed, eventualmente, 3) a singoli Moduli.  Possono essere ammessi al corso, in qualità di uditori, soggetti non in possesso del diploma di laurea magistrale o specialistica, per venire incontro alle esigenze di numerose figure professionali che si misurano quotidianamente con problemi relativi alla sicurezza informatica in ambito automazione ma che non hanno conseguito il titolo necessario all’iscrizione al Master. Tali uditori – selezionati anch’essi in base al curriculum – potranno partecipare alle lezioni e alle attività didattiche organizzate nell’ambito del Master, senza sostenere le prove di verifica e la prova finale. Al termine verrà consegnato loro un attestato di partecipazione, senza riconoscimento di crediti formativi. Agli uditori si riconosce la riduzione del 25% della quota di iscrizione all’intero Corso o ai singoli Percorsi.  Si riconosce agli iscritti agli ordini professionali, alle associazioni e ad altri enti firmatari di appositi protocolli una riduzione del 10% della quota di iscrizione all’intero Master o ai singoli percorsi. |

Piano delle Attività Formative

(Insegnamenti, Seminari di studio e di ricerca, Stage, Prova finale)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 1**  Titolo: Sistemi di Controllo Industriali (Industrial Control Systems)  Docente di rif: Chiara Foglietta | ING-INF/04 | 7 | 49 | Didattica frontale | Italiano |
| Introduzione all'Automazione Industriale. Modelli di riferimento per le reti per l'automazione. Piramide CIM e ISA 95. |  |  |  |  |  |
| PLC, architetture hardware. e software. Standard IEC 61131. Istruction List. Structured Text. LD (Ladder Diagram). FBD (Functional Block Diagram). SFC (Sequential Function Chart). |  |  |  |  |  |
| Sensori e Attuatori Industriali. Motion Control |  |  |  |  |  |
| Sistema SCADA: definizione, caratteristiche ed esempi. Base dati del processo, interfaccia operatore, Driver, Gestione allarmi, trend e rapporti, supporto alla manutenzione, sistema esperto, controllo statistico. |  |  |  |  |  |
| Safety & Security, SIL, Piping and Instrument Diagram. |  |  |  |  |  |
| Fieldbus e HART, Foundation Fieldbus, Profibus e sue versioni. Modbus e sue versioni, CANbus, Controlnet. DNP3 vs. IEC 60870, IEC 61850 per RTU. Ethernet Industriale, EtherCAT. |  |  |  |  |  |
| Wireless Sensor Network Industriale. Industrial IoT. OPC UA, Time Sensitive Network. 5G per l'industria |  |  |  |  |  |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 2**  Titolo: NORMATIVE DI RIFERIMENTO (Regulation)  Docente di rif: | ING-INF/01  ING-INF/04  ING-INF/05 | 10 | 70 | Didattica frontale | Italiano |
| Introduzione alla Cybersecurity nel mondo SCADA/ICS; Settori interessati; Casi di studio: incidenti pubblici; Hacker’s Profiling ed Agenti di Minaccia; |  |  |  |  |  |
| Introduzione a scenari correlati; Dark Web e black forums; 0days e black markets; Cyber Threat Intelligence; |  |  |  |  |  |
| NIST (National Institute of Standards and Technology) Framework for Improving |  |  |  |  |  |
| Critical Infrastructure Cybersecurity  Direttiva NIS e gli adempimenti per le infrastrutture critiche |  |  |  |  |  |
| STARTEGIA ITALIANA DI CYBER SECURITY, Perimetro Digitale |  |  |  |  |  |
| I CERT e gli CSIRT nel contesto nazionale: CERT Nazionale, CERT Agid, CERT Difesa |  |  |  |  |  |
| Minaccia cyber la sicurezza nazionale: il ruolo del CNAIPIC nella tutela delle infrastrutture critiche nel quadro della nuova architettura delineata dal decreto legislativo n. 65/2018 |  |  |  |  |  |
| ISO/IEC 27001- ISO/IEC 27002 Annex Control |  |  |  |  |  |
| NERC (North America Electric Reliability Council CIP-002/CIP-009) |  |  |  |  |  |
| Evoluzione normativa in materia di protezione dei dati |  |  |  |  |  |
| Anonimizzazione e pseudoanonimizzazione |  |  |  |  |  |
| Linee guida per IoT - approcci ENISA e NIST |  |  |  |  |  |
| Big data analytics |  |  |  |  |  |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 3**  Titolo: Technology Providers  Docente di rif: Stefano Panzieri | ING-INF/01  ING-INF/04  ING-INF/05 | 15 | 105 | Didattica frontale | Italiano |
| Beckoff - New Automation Technology |  |  |  |  |  |
| Siemens Automation |  |  |  |  |  |
| Shnaider Electrics |  |  |  |  |  |
| General Electrics |  |  |  |  |  |
| Rockwell Automation |  |  |  |  |  |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 4**  Titolo: Risk Assessment for Industrial Control Systems and Critical Infrastructures  Docente di rif: | ING-INF/01  ING-INF/04  ING-INF/05 | 6 | 42 | Didattica frontale | Italiano |
| Metodologie per l'analisi del rischio I modelli di enterprise risk management secondo gli standard ISO/IEC 27005:2011 e ISO 31000:2018 |  |  |  |  |  |
| Data Protection Impact Assessment (DPIA) |  |  |  |  |  |
| Modellistica Interdipendenze |  |  |  |  |  |
| Best Practices, OSSTMM (Open Source Security Testing Methodology Manual). ISECOM Proactive Security Square |  |  |  |  |  |
| OWASP; Secure Coding; SLD; S-SLDC |  |  |  |  |  |
| GAMP (ISPE) Pharma |  |  |  |  |  |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 5**  Titolo: Analisi del traffico e vulnerabilità (Traffic analysis and Vulnerabilities)  Docente di rif: Federica Pascucci | ING-INF/01  ING-INF/04  ING-INF/05 | 10 | 70 | Didattica frontale e di laboratorio | Italiano |
| Attachi e vulnerabilità informatiche e alcuni incidenti pubblici |  |  |  |  |  |
| Analisi traffico, IDS, network scanner, Rilevamento e gestione incidenti |  |  |  |  |  |
| Industrial IoT, 5G Security, Wireless hijacking and jamming |  |  |  |  |  |
| Attacchi livello 1 e 2, Vulnerabilità Modbus, AMS/ADS, Profinet |  |  |  |  |  |
| Attacchi livello 0 e 1, Vulnerabilità CANbus |  |  |  |  |  |
| Active and passive filtering |  |  |  |  |  |
| SCADA Forensic |  |  |  |  |  |
| Reverse Engineering, Sandboxing, Hardware Attacks |  |  |  |  |  |
| Attack and fault recognition by anomaly detection |  |  |  |  |  |
| Commercial appliances for SCADA security |  |  |  |  |  |
|  |  |  |  |  |  |
| **Titolo in italiano e in inglese e docente di riferimento** | **Settore scientifico disciplinare**  **(SSD)** | **CFU** | **Ore** | **Tipo Attività** | **Lingua** |
| **Modulo 6**  Titolo: Contromisure (Countermeasures)  Docente di rif: | ING-INF/01  ING-INF/04  ING-INF/05 | 12 | 84 | Didattica frontale e di laboratorio | Italiano |
| Crittografia nei sistemi SCADA (E2EE, OPC UA, USB control, covert channels) |  |  |  |  |  |
| IEC 62443-4-2 |  |  |  |  |  |
| Scada Filtering and Artificial Intelligence |  |  |  |  |  |
| LAB (practical experience on simulated scenarios): ICS Single Asset; ICS Base replication; ICS Complex replication; Energy power scenario; Highway scenario; Transportation scenario; Smart City scenario; Hands-on exercises; CTF challenge |  |  |  |  |  |
| SCADA Red Teaming (Attack classes, Security Assessment, Penentration testing, Vulnerability Exploiting, Shellcodes, 0days SCADA Blue Teaming (Defense classes, Cyber Threat Intelligence, Forensics, Cyber Investigations) |  |  |  |  |  |
| La sicurezza nelle Utilities |  |  |  |  |  |
| Progettazione di soluzioni per la raccolta e monitoraggio degli eventi tramite connettori (raccolta log, d.lgs. n. 231/2001, ecc.) creazione use case per obiettivi di monitoraggio eventi di sicurezza |  |  |  |  |  |

Obiettivi formativi

|  |  |
| --- | --- |
| **Attività formativa** | **Obiettivo formativo / Programma** |
| **Modulo 1** | Il modulo vuole dare una descrizione di base dei sistemi di automazione industriale e delle reti di campo da essi utilizzate. Il modulo è pensato per dare una panoramica generale dei sistemi di automazione più comuni e fornire competenze sulle modalità di programmazione dei software per PLC. A valle del modulo lo studente sarà in grado di affrontare la programmazione di semplici sistemi di controllo, coordinamento e sequenziamento di operazioni che coinvolgono macchine e sistemi di movimentazione automatici. Saranno svolte alcune esercitazioni sui software di comune utilizzo industriale. |
| **Modulo 2** | Il modulo, mira a fornire un quadro generale delle normative applicabili al mondo dell’industria 4.0 in ambito nazionale e internazionale.  Si focalizzerà in particolare sulla Direttiva NIS nota anche come Direttiva Comunitaria per la sicurezza delle reti e dell’informazione, che stabilisce i requisiti minimi di sicurezza per le reti, sistemi e servizi essenziali affidabili e sicuri, la Strategia nazionale di sicurezza cibernetica, che è un provvedimento che segna un ulteriore passo in avanti verso l’attuazione della direttiva europea, proprio per definire le procedure tecniche per la prevenzione degli incidenti cibernetici, le strutture predisposte per il loro monitoraggio quali CSRIT.  L’ultima parte del modulo pone specifica attenzione alle normative per la protezione dei dati applicabili nel contesto Industria 4.0, fornendo le linee guida per la progettazione di sistemi che rispettino i principi della minimizzazione dei dati, pseudonimizzazione e anonimizzazione nel rispetto della privacy degli individui. |
| **Modulo 3** | Questo modulo intende dare una panoramica degli approcci dei principali technology provider internazionali al problema della automazione industriale. Saranno illustrati apparati, sistemi di sviluppo, software di progettazione per reti industriali e saranno fornite indicazioni su alcuni approcci alla sicurezza industriale seguiti dalle aziende coinvolte nel modulo. |
| **Modulo 4** | La protezione dei sistemi informatici è un percorso che richiede l’adozione di diverse misure di sicurezza commisurate al rischio effettivo.  L’obiettivo del modulo è di formare professionisti che attraverso la conoscenza delle principali metodologie di analisi del rischio quali ad esempio la ISO 31000 e la conoscenza del contesto applicabile ai sistemi di controllo industriale, siano in grado di mettere ogni organizzazione nelle condizioni di individuare, prevenire e gestire tutti i rischi incombenti nell’ambito della propria attività. |
| **Modulo 5** | In questo modulo verranno affrontati i problemi di cyber-security dei sistemi di controllo industriale a partire dalle principali vulnerabilità di questi sistemi e delle reti dedicate, fino alla analisi dei principali attacchi. Saranno condotte esperienze di laboratorio per imparare ad analizzare il traffico di rete e comprendere la struttura e le vulnerabilità dei pacchetti scambiati analizzando diverse tipologie di attacchi. Sarà data enfasi alle problematiche di SCADA Forensic e Reverse Engineering e saranno mostrate tecniche di Deeep Packet Inspection per dare rilevanza semantica ai pacchetti scambiati con i controllori di campo. |
| **Modulo 6** | In questo Modulo sarà affrontato lo studio delle diverse contromisure disponibili nel settore dei controllori industriali dalla crittografia al filtraggio intelligente dei pacchetti e il monitoraggio permanente delle connessioni. Sarà affrontata l’analisi della normativa IEC62443 che rappresenta lo standard di sicurezza più importante in questo settore e saranno affrontate le tematiche della sicurezza nel settore delle Utilities dove i sistemi di IoT distribuiti pongono problemi di grande complessità. |

Stage di sperimentazione operativa

Il Master si impegna ad attivare, per i più meritevoli, stage extracurriculari, sia durante lo svolgimento del Corso che al termine di esso, nell’ambito dei numerosi Protocolli d’intesa già stipulati nonché delle nuove proposte che perverranno. La graduatoria dei meritevoli verrà formata tra gli studenti del Master in base alle votazioni ricevute negli esami sostenuti.

Percorsi Moduli didattici (solo per i Master)

Il Master è articolato in 6 moduli che rappresentano un percorso formativo coerente e per tappe in grado di portare lo studente da una conoscenza generale dei sistemi di automazione industriale fino ai problemi più complessi inerenti la sicurezza informatica di tali sistemi, passando attraverso metodologie di analisi e mitigazione del rischio che devono necessariamente essere padroneggiate da uno specialista del settore.

I percorsi didattici sottoelencati sono dei percorsi fruibili da chi ha interessi particolari e vuole approfondire solo alcuni aspetti della sicurezza dei sistemi industriali oppure vuole semplicemente avere una formazione di base per lo sviluppo di sistemi di automazione.

Nell’ambito del piano didattico del Master è quindi possibile l’iscrizione ai seguenti percorsi didattici:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Denominazione** | **Ore** | **CFU** |
| 1 | Percorso “Sistemi di Automazione Industriale” (Moduli 1 e 3) | 154 | 22 |
| 2 | Percorso “Risk management Specialist per l’Automazione” (Moduli 1, 2, 4) | 161 | 23 |
| 3 | Percorso “Cyber-security expert per l’Automazione” (Moduli 1, 3, 5, 6) | 308 | 44 |

Allo studente che avrà seguito con profitto uno o più dei percorsi didattici sopra elencati verrà rilasciato un attestato di frequenza.

Il Consiglio del Corso si riserva la possibilità di consentire l’iscrizione anche ai moduli 2, 3,4, 5, 6 (singolarmente o cumulativamente), previa verifica del possesso delle conoscenze di base, rappresentate dagli argomenti trattati nell’ambito del Modulo 1.

Tasse di iscrizione

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Importo totale** | **I rata** | **II rata** | **Scad. I rata** | **Scad. II rata** |
| Euro 4000 | 2000 | 2000 | 31 gen 2021 | 31 maggio 2021 |
| Euro 3.600 (per i soggetti iscritti ad Ordini professionali, associazioni, o altri soggetti con i quali sia stata sottoscritta apposita Convenzione) | 2000 | 1600 | 31 gen 2021 | 31 maggio 2021 |

All’importo della prima rata sono aggiunti l’imposta fissa di bollo e il contributo per il rilascio del diploma o dell’attestato.

Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l’iscrizione al Corso.

Esonero dalle tasse di iscrizione

1. È previsto l’esonero parziale delle tasse e dei contributi per gli studenti con disabilità documentata pari o superiore al 66%, che sono esonerati dal pagamento della seconda rata di iscrizione, qualora il numero totale di studenti con disabilità non sia superiore a 2. Per usufruire dell’esonero è necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.
2. Sono previste n. 7 borse di studio con esonero totale, 6 messe a disposizione da Accenture con apposita convenzione e una da fondi del Dipartimento di Ingegneria a nome del prof. Stefano Panzieri. Le borse di studio, anche quelle finanziate da enti esterni, non sono cumulabili con altri esoneri o riduzioni delle tasse e dei contributi. Altre borse di studio potranno rendersi disponibili
3. La selezione verrà effettuata tra gli studenti iscritti con le seguenti modalità:

Gli studenti che vorranno beneficiare della borsa di studio dovranno fare domanda all’atto dell’iscrizione indicando, età, occupazione attuale, data di conseguimento della laurea, Ateneo, voto finale.

Le borse vengono assegnate secondo i seguenti criteri:

1. Le borse Accenture presentano i seguenti requisiti preferenziali: laurea entro i dodici mesi precedenti all’iscrizione o non occupazione al momento dell’iscrizione.
2. La borsa di Dipartimento presenta come requisito di essere laureati presso l’Università Roma Tre.
3. È prevista l’ammissione in soprannumero di un numero massimo di 2 studenti provenienti dalle aree disagiate o da Paesi in via di sviluppo. L’iscrizione di tale tipologia di studenti è a titolo gratuito. I corsisti devono il contributo fisso per il rilascio dell’attestato finale e l’imposta fissa di bollo. Per l’iscrizione dei su citati studenti si applica quanto disposto dalla normativa prevista in merito di ammissione di studenti con titolo estero.

Tassa di iscrizione a moduli di Master

La tassa di iscrizione ai singoli percorsi/moduli è stabilita come di seguito specificato:

1. Percorso 1: euro 2000
2. Percorso 2: euro 2000
3. Percorso 3: euro 3500
4. Singolo Modulo: euro 1000

A tali importi è aggiunta l’imposta fissa di bollo. Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l’iscrizione al Corso.

Tassa di iscrizione in qualità di uditori

La tassa di iscrizione ai Corsi in qualità di uditori è fissata in euro 3000.