AISSMS
INSTITUTE OF INFORMATION TECHNOLOGY
(IOIT)
ADDING VALUE TO ENGINEERING
An Autonomous Institute Affiliated to Savitribai Phule Pune University
Approved by AICTE, New Delhi and Recognised by Govt. of Maharashtra
Accredited by NAAC with "A+" Grade | NBA - 5 UG Programmes

PROGRAM IN INSTRUMENTATION ENGINEERING

HONORS COURSE on "Advanced Industrial Automation"

STRUCTURE AND DETAIL SYLLABUS

(2025 Pattern)

AISSMS INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near RTO,
Pune – 411 001, Maharashtra State, India
Email: principal@aissmsioit.org,
Website: https://www.aissmsioit.org

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE–1.

Institute Vision & Mission

Vision:

To be recognized amongst top 10 private engineering colleges in Maharashtra by the year 2026 by rendering value added education through academic excellence, research, entrepreneurial attitude, and global exposure.

Mission :

- To enable placement of 150 plus students in the 7 lacs plus category & ensure 100% placement of all final year students.
- To connect with 10 plus international universities, professional bodies, and organizations to provide global exposure students
- To create conducive environment for career growth, prosperity, and happiness of 100% staff.
- To be amongst top 5 private colleges in Pune in terms of admission cut off

Quality Policy

We commit ourselves to provide quality education & enhance our students quality through continuous improvement in our teaching and learning processes.

Department Vision & Mission

Vision:

To be recognized as one of the best instrumentation engineering programs by developing globally competent engineers, researchers and entrepreneurs to solve real life problems through skill-based education.

Mission:

M1:To promote learning for skill-based education and emerging technologies to make students globally competent.

M2:To create conducive environment for research, innovations and entrepreneurship.

Program Educational Objectives:

Graduates will

1. solve real life problems by applying the knowledge of instrumentation technology.
2. pursue higher education or be researcher or be entrepreneur.
3. contribute as a socially responsible citizen for the development of nation.
4. for the development of nation.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Program Outcomes(POs)

1. Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. [Engineering knowledge]
2. Identify, formulate, research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. [Problem analysis]
3. Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. [Design/development of solutions]
4. Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. [Conduct investigations of complex problems]
5. Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations. [Modern tool usage]
6. Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. [The engineer and society]
7. Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. [Environment and sustainability]
8. Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. [Ethics]
9. Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. [Individual and team work]
10. Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. [Communication]
11. Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. [Project management and finance]
12. Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. [Life-long learning]

Program Specific Outcomes (PSOs)

1. Graduates will be able to apply their knowledge of measurement and control to solve the problems related to environment, safety, health and agriculture sectors.
2. Graduates will be able to demonstrate their skills on Programmable logic controller, LabView, Distributed control system and Internet of thing.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Honors Structure: Advanced Industrial Automation

Sr. No.	Course Code	Courses Name	Semester	Hrs. per week			Credit	Examination Scheme					Total
				L	T	P		ISE	ESE	TW	PR	OR	
1	INHDT511	Smart Sensors	V	03	---	--	3	40#	60*	---	---	---	100
2	INHDT512	Smart Sensors Lab	V	--	--	02	1	--	--	--	--	25	25
3	INHDT613	Advanced Communication Techniques in Instrumentation	VI	03	---	--	3	40#	60*	---	---	---	100
4	INHDT614	Advanced Communication Techniques in Instrumentation Lab	VI	--	--	02	1	--	--	--	--	25	25
5	INHDT707	Cyber Security in Automation	VII	03	--	--	3	40#	60*	---	---	---	100
6	INHDT708	Cyber Security in Automation Lab	VII	--	01	02	2	--	--	25	25	--	50
7	INHDT803	Control Room and Data Centre	VIII	03	--		3	40#	60*	--	--	--	100
8	INHDT804	Control Room and Data Centre Lab@@	VIII	--	01	02	2	--	--	25	25	--	50
			Total	12	02	08	18	160	240	50	50	50	550

*	End Semester Examination (ESE) based on subjective questions.
#	In Semester Evaluation: Insem 1: Subjective Insem 2: Based on Presentation/ Group Discussion/ Laboratory work/ Course Project/ Home Assignment/ Comprehensive Viva Voce/ Blog writing/ Case study/ Survey/ GATE based MCQ/ Numerical based subjective
Note:	@@ To earn credits, passing is mandatory in both the examination heads.

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE–1.

Third Year B.Tech Instrumentation Engineering
Smart Sensor

Course Code:	INHDT511	**Credit**	03
Contact Hours:	3 hr/week	**Type of Course:**	Lecture
Examination Scheme	In-sem. Evaluation 40 Marks	End-sem. Examination 60 Marks	

Pre-requisites: Industrial automation.

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	In-Sem. Evaluation	Internal	40
2.	End Semester Examination	External	60

Course Objectives	
1	To introduce the concept of smart sensor.
2	To provide details on MEMS.
3	To introduces sensor fabrication system.
4	To expose students to various industrial applications of smart sensors.

Course Outcomes: Students will be able to	
511.1	Identify various types of smart sensors
511.2	Differentiate micro and nanosensors
511.3	Explain sensor fabrication process
511.4	Explain advance sensing technology in smart sensors
511.5	Explain smart sensor architecture
511.6	Explain various industry applications of smart sensors.

Topics covered:

Unit I: Introduction to smart sensor (6 hrs.)

Smart sensor definition, smart sensors buses and interfaces, smart sensors for electrical and non-electrical variables, reliability of smart sensors, smart sensors software, data acquisition methods for smart sensors, signal conditioning, smart sensors for electrical and non-electrical variables, reliability of smart sensors, smart sensors software

Unit II: Smart sensor architecture (7 hrs.)

Introduction, Block diagram, types, Intelligent Sensing Techniques, sensor power management, Integration and packaging.

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Unit III: Sensor Fabrication (8 hrs.)

Design considerations and selection criterion as per standards, Sensor fabrication techniques, process details and latest trends in sensor fabrication. Thick film sensing and system design.

Unit IV: Micro and Nanotechnologies for Sensors (8 hrs.)

Fundamentals of MEMS ad NEMS, fabrication of MEMs and NEMS, microfluidics microsystems components, micromachined actuators, future trends and challenges in micro and nanosensors.

Unit V: Advanced Sensing Technology (7 hrs.)

Sensors, instruments and measurement techniques for emerging application areas such as environmental measurement like DO (dissolves oxygen), BOD (biological oxygen demand), COD (chemical oxygen demand), TOC (total organic carbon), Cox (carbon dioxides), NOx (nitrogen oxide), for navigation and inertial measurements, for agricultural measurements such as soil moisture, wind speed, leaf wetness duration, sensors for food processing like smell or odour ,taste.

Unit VI: Application and Case study (6 hrs.)

Analysis of real-world smart sensor applications, Case study in aerospace, healthcare, automotive, smart city, smart manufacturing.

Text Books:

1. Chang Liu, Foundations of MEMS, Pearson Education Inc.,2012.
2. Stephen D Senturia, Microsystem Design, Springer Publication,2000.
3. Tai Ran Hsu, MEMS & Micro systems Design and Manufacture, Tata Mc Graw Hill, New Delhi,2002.
4. Jacob Fraden, Handbook of Modern Sensors, 5 th Edition, Springer .
5. S. M. Sze, Semiconductor Sensors, Wiley 6. M J Usher, Sensors and Transducers, MacMillan,1985.

Reference Books:

1. Mohamed Gad-el-Hak, editor, The MEMS Handbook, CRC press Baco Raton,2001.
2. Julian w. Gardner, Vijay K. Varadan, Osama O.Awadelkarim, Micro Sensors MEMS and Smart Devices, John Wiley & Son LTD,2002.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Third Year B.Tech Instrumentation Engineering
Smart Sensor Lab

Course Code:	INHDT512	**Credit**	1
Contact Hours:	2 Hrs/week (P)	**Type of Course:**	Practical
Examination Scheme	Oral 25 marks		

Pre-requisites:

- Sensor and Transducer

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	Oral	External	25

Course Objectives	
1	To introduce smart sensors of industry 4.0
2	To provide details on MEMS.
3	To explain the smart sensor applications in industry.

Course Outcomes: Students will be able to	
512.1	Identify various types of smart sensors
512.2	Differentiate micro and nanosensors
512.3	Explain sensor fabrication process
512.4	Explain advance sensing technology in smart sensors
512.5	Explain smart sensor architecture
512.6	Explain various industry applications of smart sensors.

AAS

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

List of Experiments:

Students are required to perform minimum 8 program experiments from the given list.

1. Design of Signal Conditioning Circuits for Interfacing Sensors
2. To study sensor integrating system
3. To study micro sensors
4. To study nanosensors
5. To study test, calibration, and validation of electronic systems with sensors.
6. To study Off-the-shelf Data Acquisition Systems and Development Boards
7. To study power management and energy efficiency considerations for sensor systems
8. To study smart sensor 3D modelling system
9. Case study on smart sensor application in industry 4.0
10. Case study on smart sensor applications in social sustainable development.
11. Characterize the temperature sensor
12. Simulate the performance of a chemical sensor

Text Books

1. Jacob Fraden, Handbook of Modern Sensors, 5 th Edition, Springer .

References Books:

1. Mohamed Gad-el-Hak, editor, The MEMS Handbook, CRC press Baco Raton,2001.

AAS

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Third Year B.Tech Instrumentation Engineering
Advanced Communication Techniques in Instrumentation

Course Code:	INHDT613	Credit	03
Contact Hours:	3 hrs/Week	Type of Course:	Lecture
Examination Scheme	In-sem. Evaluation 40 Marks	End-sem. Examination 60 Marks	

Pre-requisites: Sensor and Transducers

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	In-Sem. Evaluation	Internal	40
2.	End Semester Examination	External	60

Course Objectives

1 To introduce fundamentals of communication techniques in instrumentation

2 To analyze and compare different communication protocols used in instrumentation.

3 To integrate various communication technologies into instrumentation systems

4 To apply security measures to protect communication systems from unauthorized access and data breaches in the context of instrumentation.

Course Outcomes: Students will be able to

613.1 Introduce fundamentals of communication techniques in instrumentation.

613.2 Explain compare different communication protocols used in instrumentation.

613.3 Explain process of integration with communication technologies into instrumentation systems.

613.4 Impart knowledge of security system in communication.

613.5 Explain industrial communication network system.

613.6 Explain device to device communication.

C
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Topics covered:

Unit I: Introduction of Communication Techniques (6 hrs.)
Basics, application, characteristics, challenges, block diagram, field level, control level, operation level

Unit II: Communication Techniques (8 hrs.)
Definition, work block diagram, standards, range, frequency band, data rate application: LoRa(Long Range), LoRaWAN(LoRa Wide Area Network), WLAN(Wireless Local Area Network), WMAN(Wireless Metropolitan Area Network), WPAN(Wireless Personal Area Network), WWAN(Wireless Wide Area Network), NB-IoT (Narrowband IoT).

Unit III: Industrial Wireless Communication (8 hrs.)
Basics, Definition, Protocol: CoAP (Constrained Application Protocol), AMQP (Advanced Message Queuing Protocol) Advanced Networking Techniques : Time-Sensitive Networking (TSN) , Software-Defined Networking (SDN) ,Machine-to-Machine (M2M) Communication

Unit IV: Industrial Communication Network (7 hrs.)
Basics, Fieldbus communication network, zero energy communication, intelligent field devices-Foundation Fieldbus(FF), Process Field Bus (PROFIBUS), Multifunction Vehicle Bus (MVB), Local Operating Network(LON) , cable and connectors.

Unit V: Communication and Security (7 hrs.)
Communication: Ethernet/IP , LiFi communication network
Security: Requirement of security, Security in industrial communication, Encryption Techniques Authentication Protocols, Access Control, Firewalls, Intrusion Detection Systems (IDS), Secure Boot, Physical Security

Unit VI: Applications in Industry 4.0 (6 hrs.)
Applications in smart manufacturing processes, chemical industry, robotic automation, Underwater Communication.

Text Books:

1. S. S. Iyengar and R. Raghavendra, Wireless Sensor Networks: Principles, Design, and Applications
2. Richard Zurawski, Industrial Communication Technology Handbook, CRC Press, ISBN-13: 978-0849319421

Reference Bools:

1. Tattamangalam R. Padmanabhan, S. K. Sinha, Industrial Instrumentation and Control Systems: Advanced Communication Techniques, CRC Press ISBN-13: 978-1420058644
2. V. C. Gungor and G. P. Hancke, Industrial Wireless Sensor Networks: Applications, Protocols, and Standards

AAS

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Third Year B.Tech Instrumentation Engineering
Advanced Communication Techniques in Instrumentation Lab

Course Code:	INHDT614	Credit	1
Contact Hours:	2 Hrs/week (P)	Type of Course:	Practical
Examination Scheme	Oral Examination 25 Marks		

Pre-requisites:

- Nil

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	Oral	External	25

Course Objectives	
1	To introduce fundamentals of communication techniques in instrumentation
2	To analyze and compare different communication protocols used in instrumentation.
3	To integrate various communication technologies into instrumentation systems
4	To apply security measures to in the context of instrumentation.

Course Outcomes: Students will be able to	
614.1	Introduce fundamentals of communication techniques in instrumentation.
614.2	Explain compare different communication protocols used in instrumentation.
614.3	Explain process of integration with communication technologies into instrumentation systems.
614.4	Impart knowledge of security system in communication.
614.5	Explain industrial communication network system.
614.6	Explain device to device communication.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

List of Experiments:

Students are required to perform minimum 8 program experiments from the given list.

1. To study communication protocol
2. To study Fieldbus Communication Setup
3. To study remote device to device communication
4. To study LoRaWAN Setup.
5. To study performance analysis of wireless network.
6. To study advanced networking techniques
7. To study fault diagnosis and troubleshoot
8. To study Industrial Ethernet Configuration.
9. To study network security simulation.
10. To study industry 4.0 application of communication techniques in instrumentation
11. Simulating wireless sensor network.
12. Setting up a Zigbee network

Text Books:

1. S. S. Iyengar and R. Raghavendra, Wireless Sensor Networks: Principles, Design, and Applications

2. Richard Zurawski, Industrial Communication Technology Handbook, CRC Press, ISBN-13: 978-0849319421

Reference Bools:

1. Tattamangalam R. Padmanabhan, S. K. Sinha, Industrial Instrumentation and Control Systems: Advanced Communication Techniques, CRC Press **ISBN-13:** 978-1420058644
2. V. C. Gungor and G. P. Hancke, Industrial Wireless Sensor Networks: Applications, Protocols, and Standards

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

B. Tech Instrumentation Engineering
Cyber Security in Automation

Course Code:	INHDT707	Credit	04
Contact Hours:	3 Hrs/Week 1 Hr/week (T)	Type of Course:	Lecture
Examination Scheme	In-sem. Evaluation 40 Marks	End-sem. Examination 60 Marks	

Pre-requisites: Sensor and Transducers

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	In-Sem. Evaluation	Internal	40
2.	End Semester Examination	External	60

Course Objectives	
1	Understand the fundamentals of cybersecurity and its significance in industrial automation.
2	Analyze cybersecurity challenges in Operational Technology (OT) networks and compare them with traditional IT security.
3	Develop incident response plans and cyber resilience strategies for industrial environments.
4	Explore emerging technologies like AI-driven cybersecurity, Zero Trust Architecture, and Blockchain in automation security.

Course Outcomes: Students will be able to	
707.1	Explain key cybersecurity concepts in industrial automation and control systems.
707.2	Implement secure network architectures using industrial security best practices.
707.3	Use risk assessment tools and threat modeling techniques to evaluate industrial cybersecurity risks.
707.4	Apply security measures such as authentication, encryption, and network segmentation in industrial environments.
707.5	Develop cyber incident response strategies and disaster recovery plans for automation systems.
707.6	Research and implement advanced cybersecurity solutions such as AI-based threat detection and Zero Trust models in automation.

AAS

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS)
PUNE-1.

Topics covered:

Unit I: Introduction to Cybersecurity in Automation (6 hrs.)
Overview of Cybersecurity and its Importance in Automation, Threat Landscape in Industrial Automation Systems, Cybersecurity Challenges in Operational Technology (OT) vs. IT, Industrial Control Systems (ICS) and Their Vulnerabilities.

Unit II: Industrial Automation and Control Systems (IACS) Security (8 hrs.)
Introduction to Industrial Automation and Control Systems (IACS), Security Threats in PLCs, SCADA, and DCS Systems, Cybersecurity Risks in Robotics and Smart Manufacturing, Industry 4.0 and Security Considerations.,

Unit III: Cyber Threats and Attack Vectors in Automation (8 hrs.)
Malware and Ransomware Attacks on Industrial Systems, Insider Threats and Human Factor Risks, Case Studies on Cyber Attacks (Stuxnet, Triton, BlackEnergy), Understanding Zero-Day Vulnerabilities and Exploits

Unit IV: Secure System Design and Hardening Techniques (7 hrs.)
Security-by-Design for Industrial Automation, Hardening PLCs, SCADA, and Industrial IoT Devices, Secure Coding Practices for Automation Software, Patch Management and Firmware Security.

Unit V: Emerging Technologies and Trends in Cybersecurity for Automation (7 hrs.)
Role of AI and Machine Learning in Industrial Cybersecurity, Blockchain for Secure Industrial Transactions, Zero Trust Architecture in OT Security, Future of Cybersecurity in Smart Factories.

Text Books:

1. Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS" – Tyson Macaulay & Bryan L. Singer

2. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment" – Pascal Ackerman

3. "Cybersecurity in Industrial Automation and Control Systems" – Edward J. M. Colbert & Alexander Kott

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE–1.

B. Tech Instrumentation Engineering
Cyber Security in Automation Lab

Course Code:	INHDT708	**Credit**	**1**
Contact Hours:	2 Hrs/week (P)	**Type of Course:**	Practical
Examinatio nScheme	Term work Examination 25 Marks	Practical Examination 25 Marks	

Pre-requisites:

- Sensor and Transducer

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	Termwork	Internal	25
2	Practical	External	25

Course Objectives

1	Understand the fundamentals of cybersecurity and its significance in industrial automation.
2	Analyze cybersecurity challenges in Operational Technology (OT) networks and compare them with traditional IT security.
3	Develop incident response plans and cyber resilience strategies for industrial environments.
4	Explore emerging technologies like AI-driven cybersecurity, Zero Trust Architecture, and Blockchain in automation security.

Course Outcomes: Students will be able to

708.1	Explain key cybersecurity concepts in industrial automation and control systems.
708.2	Implement secure network architectures using industrial security best practices.
708.3	Use risk assessment tools and threat modeling techniques to evaluate industrial cybersecurity risks.
708.4	Apply security measures such as authentication, encryption, and network segmentation in industrial environments.
708.5	Develop cyber incident response strategies and disaster recovery plans for automation systems.
708.6	Research and implement advanced cybersecurity solutions such as AI-based threat detection and Zero Trust models in automation.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

List of Experiments:

Students are required to perform minimum 5 modules from the given list.

Module 1: Introduction to Industrial Cybersecurity

1. Understanding Cybersecurity in Automation
   - Explore vulnerabilities in PLC, SCADA, and industrial networks.
   - Identify potential cyber threats in automation environments.
2. Configuring a Virtualized Industrial Network for Security Testing
   - Set up a virtual ICS/SCADA lab using tools like Factory I/O, Matrikon OPC, or Cyber Range.
   - Simulate an industrial control environment for security analysis.

Module 2: Industrial Network Security & Secure Communication

3. Network Traffic Analysis for ICS/SCADA Security
   - Use Wireshark to analyze Modbus, OPC-UA, and MQTT traffic.
   - Identify abnormal activities or unauthorized access.
4. Implementing Firewall and Network Segmentation for OT Security
   - Configure firewalls (pfSense, Cisco ASA) and VLAN segmentation for an industrial network.
   - Isolate critical automation components from IT systems.
5. Intrusion Detection System (IDS) for ICS Security
   - Set up Snort or Suricata to detect cyber threats in industrial networks.
   - Create custom rules to detect unauthorized PLC access.

Module 3: Securing SCADA, PLCs & Industrial Devices

6. Hardening a PLC Against Cyber Threats
   - Secure a PLC (Siemens, Allen-Bradley) by disabling unused ports, configuring authentication, and updating firmware.
7. Simulating a Cyber Attack on a SCADA System
   - Perform a simulated Man-in-the-Middle (MITM) attack on a SCADA network and analyze logs.
8. Configuring Secure Remote Access for Industrial Automation
   - Set up VPN or SSH-based secure remote access to industrial controllers.

Module 4: Threat Detection, Incident Response & Risk Assessment

9. Performing a Risk Assessment for an Industrial Control System
   - Conduct vulnerability assessment using tools like OpenVAS or Nessus.
   - Identify security gaps and recommend mitigation strategies.
10. Responding to a Cybersecurity Incident in an Automation System
   - Simulate an ICS ransomware attack scenario and implement response actions.
11. Malware Detection in Industrial Systems
   - Use YARA rules to detect malware in PLC/SCADA software.

Module 5: Compliance & Security Standards for Automation

12. Implementing IEC 62443 Cybersecurity Best Practices
   - Configure a sample ICS environment to align with ISA/IEC 62443 security zones.
13. Ensuring Regulatory Compliance in an Industrial Network
   - Audit an industrial system for compliance with NIST, NERC-CIP, or GDPR standards.

Module 6: Advanced Security & Future Technologies in Automation

14. Using AI for Threat Detection in Industrial Networks
   - Deploy AI-driven cybersecurity tools (e.g., Splunk, Darktrace) to detect anomalies in OT traffic.
15. Blockchain for Secure Industrial Transactions
   - Implement a blockchain-based identity verification system for secure automation transactions
16. Developing a Cybersecure Industrial Automation System
   - Design a fully secured industrial automation setup, implementing best security practices.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Text Books:

1. Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS" – Tyson Macaulay & Bryan L. Singer
2. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment" – Pascal Ackerman
3. "Cybersecurity in Industrial Automation and Control Systems" – Edward J. M. Colbert & Alexander Kott

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE–1.

B.Tech Instrumentation Engineering Control Room & Data Centre			
Course Code:	INHDT803	Credit	04
Contact Hours:	3 Hrs/Week 1 Hr/week (T)	Type of Course:	Lecture
Examination Scheme	In-sem. Evaluation 40 Marks	End-sem. Examination 60 Marks	

Pre-requisites: Nil

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	In-Sem. Evaluation	Internal	40
2.	End Semester Examination	External	60

Course Objectives	
1	Understand the fundamental principles of control rooms and data centers in industrial and IT environments.
2	Learn about the design, layout, and ergonomic considerations for efficient control room operations.
3	Gain knowledge of data center infrastructure, including power management, cooling systems, and network architecture.
4	Study data center virtualization, cloud computing, and edge computing for modern enterprise needs.

Course Outcomes: Students will be able to	
803.1	Explain the core functions and components of control rooms and data centers.
803.2	Design and optimize data center infrastructure, including power, cooling, and network security.
803.3	Implement best practices for control room and data center layout, redundancy, and reliability.
803.4	Apply virtualization, cloud computing, and hybrid data center models for optimized performance.
803.5	valuate emerging technologies, such as AI-driven monitoring, edge computing, and sustainable data centers.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Topics covered:
Unit I: Introduction to Control Rooms and Data Centres (6 hrs.) Overview of Control Rooms and Data Centres in industrial and enterprise environments, Importance of Mission-Critical Infrastructure, Difference between Industrial Control Rooms & IT Data Centres, Evolution of Smart Control Rooms and Data Centre Automation.
Unit II: Control Room Infrastructure & Design (8 hrs.) Physical Layout and Ergonomics of a Control Room, Human-Machine Interface (HMI) & SCADA Systems in Control Rooms, Video Walls, Workstations, and Communication Systems, Control Room Security & Surveillance Systems, Case Studies: Best Practices in Modern Control Room Design.
Unit III: Data Centre Infrastructure & Components (8 hrs.) Data Centre Tiers & Standards (Uptime Institute Tier I-IV), Components of a Data Centre: Servers, Storage, Networking Equipment, Rack Management & Cable Management Best Practices, Power and Cooling Systems in Data Centres (UPS, HVAC, CRAC, Liquid Cooling), Environmental Monitoring & Fire Suppression Systems.
Unit IV: Networking & Communication in Control Rooms & Data Centres (7 hrs.) Industrial Networks (ICS/SCADA) vs. Enterprise Data Center Networks, Redundancy & High Availability Strategies (Failover, Load Balancing), Data Centre Protocols (Ethernet, TCP/IP, Fiber Channel), 5G & Edge Computing in Control Rooms & Data Centres.
Unit V: Emerging Technologies & Future Trends (7 hrs.) AI & Machine Learning for Control Room Automation, Blockchain for Secure Data Centre Operations, Quantum Computing & Its Impact on Data Centres, Future Trends in Control Room & Data Centre Management.

Text Books:

1. Control Room Design Guide" – Peter B. Kidger
2. Designing & Building Control Rooms: A Guide to Infrastructure and Ergonomics" – David W. Gilmore
3. Data Center Virtualization Fundamentals" – Gustavo A. A. Santana
4. AI and Machine Learning for Control Room Operations" – James P. Lux

AAS

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

B. Tech Instrumentation Engineering
Control Room and Data Centre Lab

Course Code:	INHDT804	**Credit**	1
Contact Hours:	2 Hrs/week (P)	**Type of Course:**	Practical
Examination Scheme	Termwork Examination 25 Marks	Practical Examination 25 Marks	

Pre-requisites:

- Nil

Course assessment methods/tools:

Sr. No.	Course assessment methods/tools	External/ Internal	Marks
1.	Termwork	Internal	25
2	Practical	Externa l	25

Course Objectives	
1	Understand the fundamental principles of control rooms and data centers in industrial and IT environments.
2	Learn about the design, layout, and ergonomic considerations for efficient control room operations.
3	Gain knowledge of data center infrastructure, including power management, cooling systems, and network architecture.
4	Study data center virtualization, cloud computing, and edge computing for modern enterprise needs.

Course Outcomes: Students will be able to	
804.1	Explain the core functions and components of control rooms and data centers.
804.2	Design and optimize data center infrastructure, including power, cooling, and network security.
804.3	Implement best practices for control room and data center layout, redundancy, and reliability.
804.4	Apply virtualization, cloud computing, and hybrid data center models for optimized performance.
804.5	valuate emerging technologies, such as AI-driven monitoring, edge computing, and sustainable data centers.

CHAIRMAN
BOS-INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

List of Experiments:

Perform any 5 Module from given list

Module 1: Introduction to Control Rooms & Data Centers

1. Understanding Control Room & Data Center Components
   - Identify key elements such as workstations, video walls, HMI, network racks, cooling systems, and power distribution.
   - Study different control room layouts (Industrial, Process Control, Security, and IT Operations).
2. Setting Up a Virtual Control Room & Data Center Environment
   - Use simulation software (Factory I/O, SCADA simulators, Packet Tracer) to create a virtual control room.
   - Set up a basic virtual data center environment with VMware, Hyper-V, or Proxmox.

Module 2: Control Room & Industrial Network Security

3. SCADA & PLC Communication Analysis
   - Configure and analyze SCADA/PLC protocols (Modbus, OPC-UA, MQTT) using Wireshark.
   - Identify cybersecurity vulnerabilities in SCADA communication.
4. Configuring a Secure Industrial Network for a Control Room
   - Set up firewalls (pfSense, Cisco ASA) and VLAN segmentation for OT/IT separation.
   - Implement role-based access control (RBAC) in SCADA/HMI systems.
5. Intrusion Detection in Industrial & Data Center Networks
   - Deploy Snort or Suricata IDS in a simulated control room or data center.
   - Monitor and analyze network traffic for potential cyber threatModule 3: Data Center Infrastructure & Power Management
6. Rack & Cable Management in a Data Center
   - Design a server rack layout and implement structured cable management.
   - Use software tools (NetBox or Visio) for data center topology design.
7. Power & Cooling System Configuration in a Data Center
   - Set up UPS and Power Distribution Unit (PDU) simulation.
   - Monitor energy efficiency and cooling strategies (CRAC, Liquid Cooling, Free Cooling).

Module 4: Virtualization, Cloud, and Edge Computing

8. Deploying Virtual Machines in a Data Center
   - Use VMware, VirtualBox, or Hyper-V to create a virtualized environment.
   - Configure server clustering, load balancing, and storage virtualization.
9. Setting Up a Hybrid Cloud Infrastructure
   - Integrate on-premises data center with cloud platforms (AWS, Azure, Google Cloud).
   - Implement containerization using Docker/Kubernetes.
10. Edge Computing Deployment for Smart Control Rooms

- Set up edge computing nodes for real-time data processing in industrial environments.
- Deploy an IoT-based monitoring system using Raspberry Pi or NVIDIA Jetson.

Module 5: Cybersecurity & Compliance in Data Centers & Control Rooms

11. Performing a Risk Assessment for a Data Center or Control Room

- Use NIST Cybersecurity Framework or IEC 62443 for risk analysis.
- Identify security vulnerabilities and suggest mitigation strategies.

12. Implementing Identity & Access Management (IAM) in a Control Room

- Set up Multi-Factor Authentication (MFA) for SCADA or data center access.
- Configure Active Directory (AD) and Role-Based Access Control (RBAC).

13. Disaster Recovery & Business Continuity Planning (BCP/DRP) Simulation

- Simulate a cyber attack or power failure scenario in a data center.
- Implement and test a disaster recovery plan using backup & failover strategies.

Module 6: AI & Emerging Technologies in Control Rooms & Data Centers

14. AI-Powered Monitoring for Control Rooms & Data Centers

- Implement AI-based monitoring tools (Splunk, Darktrace) for anomaly detection.
- Analyze real-time alerts and response mechanisms.

15. Blockchain for Secure Data Center Transactions

- Set up a basic blockchain-based identity verification for access control.
- Explore smart contracts for secure industrial transactions.

Design & Implement a Fully Secured Smart Control Room or Data Center

- Create a comprehensive control room/data center setup with best security and performance practices.
- Present a detailed risk assessment and future scalability plan.

CHAIRMAN
BOS INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE-1.

Text Books:

1. Control Room Design Guide" – Peter B. Kidger
2. Designing & Building Control Rooms: A Guide to Infrastructure and Ergonomics" – David W. Gilmore
3. Data Center Virtualization Fundamentals" – Gustavo A. A. Santana
4. AI and Machine Learning for Control Room Operations" – James P. Lux

CHAIRMAN
BOS–INSTRUMENTATION ENGINEERING
AISSMS IOIT (AUTONOMOUS),
PUNE–1.