DEPARTMENT OF INSTRUMENTATION AND CONTROL ENGINEERING

COURSE PLAN – PART I			
Name of the Programme and specialization	**M. Tech , Industrial Automation**		
Course Title	**Cyber Security in Industrial Automation**		
Course Code	**IC 613**	**No. of Credits**	**3**
Course Code of Pre-requisite subject(s)	**Nil**		
Session	**July 2020**	**Section**	**NA**
Name of Faculty	**Dr. Sunil Shah Guest Faculty**	**Department**	**ICE Guest Faculty**
Official Email	**sunil.shah@modelicon.in**	**Telephone No.**	**9245057005**
Name of Course Coordinator(s)	**Dr. M. Umapathy, Professor HAG**		
Official E-mail	**umapathy@nitt.edu**	**Telephone No.**	**9443013136**
Course Type (please tick appropriately**)**	☐ **Elective course**		

Syllabus (approved in BoS)

Course Content

Industrial Automation Fundamental Concepts - Industrial automation protocol summary-The Open System Interconnection(OSI) Model, The Transmission Control Protocol (TCP)/ Internet protocol (IP) Model, Object linking and embedding for process control, Open platform communication(OPC) Unified architecture, Modbus/ TCP Model, The distributed network protocol, Controller area network, Ethernet/ IP, Open safety protocol

Information System Security Technology- Types and classes of attack, Policies, Standards, Guidelines and procedures, Malicious code and attacks, Firewalls, Cryptography, Attacks against cryptosystems.

Industrial Automation Culture versus Information Technology (IT) Paradigms- Considerations in adapting IT security methods to industrial automation, Threats, IT and industrial automation.

Risk Management for Industrial Automation- Risk management, ANSI/ISA-62443-2-1 (99.02.01)-2009 cyber security, Risk analysis, Addressing risk, NIST SP 800-39 Integrated enterprise risk management, Threats.

Industrial Automation Trends, Approaches, and Issues- Automation trends, Formal methods used to quantify and standardize, Important concepts and applications- Information security continuous monitoring (ISCM) strategy, The Smart Grid Maturity Model (SGMM), Future smart grid issues and automation security issues.

Emerging Approaches to Industrial Automation Security- Internet of Things, Open platform communications unified architecture, Security and privacy, Big data analytics and the industrial Internet of Things, The National Institute of Standards Technology (NIST) Cyber-Physical Systems (CPS) Framework, CPS and Cybersecurity, Critical Infrastructure security, Software-defined elements.

Text Books

1. *Ronald L. Krutz, "Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure", 2nd Edition, International Society of Automation, 2017.*
2. *David J. Teumim, "Industrial Network Security, Second Edition", International Society of Automation, 2010.*

Reference Books

1. *Lawrence M. Thompson and Tim Shaw, "Industrial Data Communications", Fifth Edition, International Society of Automation, 2015.*
2. *Dick Caro, "Automation Network Selection: A Reference Manual", 3rd Edition, Paperback, International Society of Automation, 2016.*

COURSE OBJECTIVES

1. To introduce the knowledge industrial communication and their relevance in cyber security
2. Understand the importance of security implementation in Industrial Control Systems and difference in Security requirements for Information Technology and Operation Technology
3. Understand the various security threats and vulnerabilities of the cyber world keeping in line with the industrial trends.
4. Understand risk management requirements for ICS and relevant standards
5. Understand the emerging trends in automation, IOT, IIOT and increasing risks for ICS

MAPPING OF COs with POs	
Course Outcomes On completion of the course, the student will be able to,	**Programme Outcomes (PO)** **(**Enter Numbers only**)**
1. Get knowledge of security mechanisms, standards and state-of–the-art capabilities.	**1, 2**
2. Design new systems and infrastructure level security solutions.	**3, 4**
3 develop and maintain new tools and technologies to enhance the security of applications in industrial automation.	**4**
4. Identify and solve different cyber security threats.	**5**

COURSE PLAN – PART II			
COURSE OVERVIEW			
This course introduces the basic and advanced concept of cyber security systems and issues in Industrial Automation.			
COURSE TEACHING AND LEARNING ACTIVITIES			
S.No.	**Week/Contact Hours**	**Topic**	**Mode of Delivery**
1	6	Industrial Automation Concepts. Industrial Communication	Lectures, Demonstrations, Hands-on Sessions
2	7	Information System Security Technology, Cryptography	Lectures, Demonstrations, Hands-on Sessions
3	2	Industrial Automation Culture versus Information Technology (IT) Paradigms	Lectures, Demonstrations, Hands-on Sessions
4	10	Risk Management for Industrial Automation	Lectures, Demonstrations, Hands-on Sessions

5	12	Emerging Approaches to Industrial Automation Security	Lectures, Demonstrations, Hands-on Sessions, Invited Lectures
6	8	ICS cybersecurity concepts deep dive	Presentations by students

COURSE ASSESSMENT METHODS (shall range from 4 to 6**)**

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1.	Assessment I: Open Book MCQ	28 Oct	30 min	15 %
2	Assessment II: Open Book MCQ	25 Nov	30 min	15 %
3	Assessment III: Student presentations	21/25 Nov	8 hrs (20 min each group)	20 %
4	Assessment IV: Hands on sessions	Continuous	-	20 %
5	Final Assessment *		2 hours	30 %

***mandatory; refer to guidelines on page 4**

COURSE EXIT SURVEY (mention the ways in which the feedback about the course shall be assessed)

Feedback from students will be obtained during the course Students' performance in test and their presentation during discussion will be used to assess the understanding level.

COURSE POLICY (including compensation assessment to be specified**)**

1.75% of attendance is must, inclusive of On duty on any grounds. 5% of relaxation can be considered on medical grounds. Students not acquiring the required attendance will be assigned V grade.

2. Relative grading with passing minimum of 40 % or clustering will be followed, on seeing the overall performance of the students and if the class strength is less than 10 absolute grading policy will be followed.

3. For the students missing the assessment for medical reasons, one compensation assessment will be conducted one week before the final assessment for a weightage, equal to that of the missed assessments. But students are advised not to miss the assessments.

4 For the students not passing the course, reassessment will be conducted during the first week of next semester for a weightage of 100% and the grades will be given on absolute grading policy.
6. For academic dishonesty institute policy will be followed. As assessments are happening online students are advised not to practice copying, plagiarism check will be happening.

ADDITIONAL INFORMATION, IF ANY

NIL

FOR APPROVAL

Course Faculty/ Co-originator	CC- Chairperson	HOD