Course Description:
Due to increasing connectivity of industrial automation and control systems (IACS) the relationship between safety, security, and alarm management in control systems has never been more important than now. This course introduces the integrated automation lifecycle approach for meeting the requirements for the IEC 61511 (safety) and IEC 62443 (IACS cybersecurity) standards. Covered topics include: fundamentals of the functional safety and cybersecurity principles for: risk analysis, safety/cybersecurity requirement specifications, inherently safer/secure design techniques, Safety Integrity Level (SIL) / Security Level (SL) verification, requirements for operations and maintenance, and discussion of real-world cybersecurity attacks.

Prerequisites:
Elec Eng 3340 or Ch Eng 4110
Credit Hours:  LEC 3   LAB 0

Week  Tentative Course Topics
1   Introduction to Safety Instrumented Systems, Principles of Risk Management
2   The Safety Lifecycle, Process Hazard Analysis (PHA)
3   Consequence Analysis, Likelihood Analysis
4   Layer of Protection Analysis (LOPA)
5   Tolerable Risk, SIL Target Selection, Safety Requirements Specification (SRS)
6   Safety Instrumented Systems (SIS) failure, From failure rate to SIL, Single devices to system
7   Redundant Architectures, Requirements to safety instrumented function (SIF), SIF Design and Verification in the Safety Lifecycle
8   SIF Detail Design, Operations
9   Relevant industrial automation and control systems (IACS) security standards, Assessing IACS cybersecurity, Best practices for developing security policy, procedures, and standards,
10  Conducting High-Level and Detailed Cybersecurity Risk Assessments
11  Completing Cybersecurity Requirement Specification, Best practices for providing access control, Best practices for system hardening
12  Cybersecurity lifecycle - Assessment, Design & Implementation, and Operation & Maintenance, best practices for monitoring your control systems.
13  Incident Response, Business Continuity Planning, Periodic Vulnerability Assessments, and Management of Change
14  Understanding and Applying the Integrated Automation Lifecycle Approach
15  Alarm management practices and principles
This course will be taught online, using existing courses or parts of courses already offered online by Exida in these subject areas. The S&T instructor (Dr. Erickson) will coordinate the course, but the content will be taught by Exida engineers.

There will be weekly online quizzes over the lectures for that week. In addition, the students will write 2 papers. The first paper will be either a simple SRS (safety requirements specification), a simplified SIL verification calculation, or a root cause analysis of an incident in industry with recommendations (combination of organizational changes and/or instrumentation changes), the second paper will assess the cybersecurity risks to the Factory Automation Laboratory at S&T and propose changes as needed to meet IACS security standards.

The course grade will be based on the weekly quizzes and the two papers.