The purpose of any educational undertaking is to create an experience that results in a cognitive change in students. For most, this will take the form of the new knowledge and skills required for their work roles. Based on the content areas identified in Figure 1, we developed the following learning outcomes to articulate what students graduating from programs in ICSS should know and be able to do:

1. Maintain ICS devices and attendant networks
2. Identify and mitigate evolving ICS security threats
3. Assess evolving risks to ICS systems
4. Maintain high standards of safety in ICS environments
5. Implement and maintain ICSS software
6. Communicate with OT and IT personnel

CSS programs. These programs will differ in both their length and the level of expertise of the learners they serve. Therefore, we have attempted to create a basic program structure that can be adapted for multiple levels of expertise and program length. This program structure addresses ICSS in five basic areas. This differs from the topic areas outlined above in Figure 1 because it groups these topics into units that make more sense for students when constructing a learning experience/mental model of the discipline. Having reviewed the major areas and major concepts, and having discussed the way that expertise in ICSS develops with subject matter experts in the field – we propose the following five knowledge areas:

1. Risk
2. Governance/Compliance
3. Information Security
4. ICS
5. Electrical Engineering

For additional information regarding this research, please contact Douglas Rapp at rapp1@purdue.edu