Machine Learning Text Classification and Natural Language Processing Approach to Cybersecurity Training Curriculum Analysis

August 2021

Team Boilermaker

Kevin Tian  
*Purdue University*  
West Lafayette, Indiana, USA  
tian160@purdue.edu

Bengisu Cuneyit  
*Purdue University*  
West Lafayette, Indiana, USA  
bcuneyit@purdue.edu

INL Mentor

Dr. Gary M. Deckard  
gary.deckard@inl.gov
Abstract

In the domain of cybersecurity, there are a wide variety of education and training courses offered by a variety of training providers (commercial vendors, governmental, and academic institutions). Unfortunately, a comprehensive cross-provider mapping of the body of course offerings does not currently exist. Furthermore, although individual providers have made efforts, an accepted cross-provider mapping of education and training courses (or categories) to an accepted framework of work-roles by cybersecurity work-role and competency level has not yet been developed. The inability to compare training courses by topic or cybersecurity work-role and the level of difficulty (competency level) affects all organizations in identifying and selecting potential training opportunities for personnel performing cybersecurity duties.

In this work, we report on our application of Machine Learning (ML) Text Classification and Natural Language Processing (NLP) methodologies to begin to create a process to organize an accurate and thorough catalog of course offerings by work-role and competency level. Through the analysis of text-based course attributes (description, learning objectives, prerequisites, etc.), along with the text-based attributes for identified cybersecurity work-roles, our ML efforts examined methods to determine the work-role “best-fit” for each course, as well as the competency level through action-verb text comparison.
# Table of Contents

I. Table of Contents .................................................................................................................. 3

II. Introduction .......................................................................................................................... 4

III. Related Work ....................................................................................................................... 5

IV. Methodology ......................................................................................................................... 6

A. Phase 1 .................................................................................................................................. 6

B. Phase 2 .................................................................................................................................. 7

V. Results and Discussion .......................................................................................................... 7

A. Phase 1: Naïve Bayes (NB) & Support Vector Machines (SVM) Approach ....................... 7

1. Accuracy .............................................................................................................................. 7

2. Interpretation of Confusion Matrix ...................................................................................... 8

B. Phase 2: Cosine Similarity & Euclidean Distance ............................................................... 9

VI. Conclusions ......................................................................................................................... 10

VII. Future Work ....................................................................................................................... 11

VIII. References ......................................................................................................................... 12

Appendix A – COSTAR Analysis and 5-Minute Brief ............................................................ 15

Appendix B – Code Repository .............................................................................................. 17

Appendix C – Detailed Figures & Results .............................................................................. 35

Appendix D – External Programs .......................................................................................... 50
II. Introduction

Many employees in the cybersecurity workforce today perform additional tasks outside the scope of their original job description. As the cybersecurity field evolves to encompass a wider variety of job duties, it becomes more difficult to hire the necessary workforce and train current employees for all tasks that they need to perform. Many positions in the cybersecurity workforce have common duties as well as other basic requirements, such as education and experience. This blurs the lines between distinct “specialized” jobs and limits growth opportunities within corporations, which in return can demotivate employees and discourage them from expanding their skillsets.

Organizations face numerous challenges in hiring cybersecurity talent as well as educating and training their cybersecurity workforce to meet the needed competency levels required for specific cybersecurity work-roles. Additionally, organizations struggle to understand the specific training needed for their workforce and to justify expenditure of training funds without comparative references between potential training offerings. A major factor is the lack of standardization in cybersecurity education and training standards for curriculum. This task is particularly difficult for the cybersecurity workforce tasked with protecting the Industrial Control Systems (ICS) systems that operate our nation’s critical infrastructure.

In this work, we applied Machine Learning (ML) Text Classification methodologies to organize an accurate and thorough catalog of course offerings that establishes competency level equivalencies across providers. We theorized that it was possible to align the course offerings to an accepted framework of industry work-roles such as the National Institute for Standards & Technology (NIST) National Initiative for Cybersecurity Education (NICE) (Petersen, Santos, Smith, & Witte, 2020) by work-role and competency level. While the NIST NICE Framework does not include a work-role framework for ICS cybersecurity, joint research between Idaho National Laboratory (INL) and Idaho State University (ISU) has proposed standardized cybersecurity work-roles for the ICS field. As we discuss the goals of our project, consider that the discussion of “work-roles” includes those in ICS-related areas. To manually tag and label courses currently, courses must be categorized by subject matter experts or through expert analysis.

Training offerings across the cybersecurity field have associated course descriptions with specific text-based attributes for each course. Correspondingly, the NICE Framework and ISU-INL research driven ICS work-roles contain text-based descriptions and verbiage for their associated Tasks, Knowledge, and Skills (TKSs).¹

The overall significance of our research lies in the novelty of utilizing ML to classify work-role frameworks and cybersecurity curriculum descriptions in a way whereby organizations which have assigned specific work-roles for their cybersecurity workforce can then identify appropriate training by work-role and competency level, regardless of provider or instructional method (Deckard, 2021).

¹ Skill and Ability statements from the previous NICE Framework version have been refactored for simplicity into Skill statements.
III. Related Work

Our project concept is grounded in recent course equivalency work by the Federal Emergency Management Agency (FEMA) and Argonne National Laboratory (ANL) to map course equivalencies for State, Local, Tribal & Territorial (SLTT) training courses to existing FEMA courses. This work relied upon decision science techniques such as multi-attribute utility theory (MAUT) (Jansen, 2011), Natural Language Processing (NLP) (IBM, 2020), and the concepts of ML text classification to understand the meaning of various text-based attributes for each course. Through this work, FEMA and ANL were able to create a Course Equivalency Tool (CET) to evaluate courses and assign equivalencies (Argonne National Laboratory, 2020). This tool uses a course equivalency model that measured the similarity of courses through three different approaches: course match, course methodology, and course topic.

Another work that contributed significantly to this project was the unpublished master’s thesis work of Randall Jung, a research fellow at INL. Jung’s work utilized the NICE framework to show how the federal government’s General Schedule system (GS) failed to maintain currency, specifically for the GS-2210 job series. The NICE framework utilizes ‘task,’ ‘knowledge,’ and ‘skill’ statements in conjunction with ‘work’ and ‘learner’ concepts to categorize employee competencies and outline a standardized method of describing work-roles (Jung, 2020). Accompanying the master’s thesis, Jung included a training course repository with cybersecurity courses manually categorized into NICE roles and Bloom’s Taxonomy Levels (Armstrong, 2010), among other labels.

The Competency Health and Maturity Progression Model (Cyber-CHAMP) is a five-step model created and developed at INL to provide Cyber awareness and training to improve an organization’s cyber efficiency (Hott, Stailey, Haderlie, & Ley, 2020). Cyber-CHAMP hopes to address the issue of organizations without a standardized communication framework, introducing the term ‘cyber-hygiene’. The five steps include taking a snapshot of the organization’s cyber hygiene, mapping the organization’s job positions and job roles, having employees complete a task analysis worksheet, and producing training recommendations for employees based on their task analysis results, and reassessing the organization’s cyber hygiene after a period of time.

Cyber-CHAMP includes a Task Analysis Tool, which prompts the user about various skills and tasks typically used in their work, eventually giving the user a breakdown of how their skills align within the context of the NICE framework. In addition to this breakdown, the tool also offers a list of manually aggregated cybersecurity training courses pertaining to an employee’s areas of skill. The current methodology of course recommendation is a significant weakness within the Cyber-CHAMP tool, as this manual method will not scale well with the increase of courses, and the course list offered does not consider the user’s competency level.

We believe many of these issues with the previous methodology can be rectified through a machine learning algorithm/script that will categorize cybersecurity courses and create an indexable catalog that will pair users with relevant cybersecurity courses for their specific competency level.
IV. Methodology

The data used in this paper primarily comes from Randall Jung’s repository of cybersecurity courses included with the master’s thesis (Jung, 2020). The repository is a Microsoft Excel workbook organized into different spreadsheets. The sheet we primarily focused on is the ‘Trainings’ sheet, where each training course was labeled by the course vendor, classification status, course number, course title, course description, Bloom’s Taxonomy Level, etc. (For full spreadsheet see Table C1). In total, the dataset has 18 categories, with some of the data entries missing. These courses constituted the ‘main dataset’ of training courses our model trained on and was augmented by the manually aggregated course catalog currently used in the Cyber-CHAMP Task Analysis Tool.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Course Number</th>
<th>Course Title</th>
<th>Course Description</th>
<th>Course Duration</th>
<th>Course Cost</th>
<th>Course Delivery</th>
<th>Course Location</th>
<th>Access Period</th>
<th>Competency Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>5A</td>
<td>FGDE</td>
<td>Mathematics for Instrumentation Technicians</td>
<td>This course is specifically designed for the Instrument technician who may be struggling with mathematical computations or those who need a basic refresher. The course is focused entirely on fundamental problems and solutions that an Instrument technician needs with form entry to supervisory level experience. It also provides a good prerequisite for the various math calculations involved in other GA training courses.</td>
<td>8-10 days</td>
<td>$2,500</td>
<td>Live</td>
<td>Live</td>
<td>6-8 weeks</td>
<td>Fundamentals</td>
</tr>
<tr>
<td>5A</td>
<td>FIBF</td>
<td>Intro to Industrial Processes, Measurement and Control</td>
<td>This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Careers, engineers, and managers are provided with a foundation for communication with other control system professionals, serves as a solid fundamental course for introduction to other GA courses.</td>
<td>8 days</td>
<td>1,200</td>
<td>Live</td>
<td>Live</td>
<td>4-6 weeks</td>
<td>Fundamentals</td>
</tr>
<tr>
<td>5A</td>
<td>FGDE</td>
<td>Fundamentals of Industrial Process Measurement &amp; Control</td>
<td>This self-paced, online course provides an overview of industrial measurement and control for technicians, engineers, and managers providing a basic understanding and foundation for communication with other control systems professionals.</td>
<td>11 weeks</td>
<td>2,000</td>
<td>Online</td>
<td>Online</td>
<td>12-16 weeks</td>
<td>Fundamentals</td>
</tr>
<tr>
<td>5A</td>
<td>FGDE</td>
<td>Developing and Applying Standard Instrumentation and Control Documentation</td>
<td>This course will present the methodology for the designing and developing of control systems documentation. The development of piping and instrument diagrams (P&amp;ID) and related GA drawings are emphasized. This course concentrates on the development and the reading/interpreting of these documents, making beneficial to engineers, designers, software engineers, system integrators, and technicians.</td>
<td>2 days</td>
<td>1,200</td>
<td>Live</td>
<td>Live</td>
<td>2-4 weeks</td>
<td>Novice</td>
</tr>
</tbody>
</table>

Figure 1: ‘Trainings’ spreadsheet in Randall Jung’s repository of cybersecurity courses

In the process to organize cybersecurity courses, we treated each course as a ‘document,’ allowing our process to closely align to traditional document classification techniques within the NLP space. Due to time constraints and the popularity of Naïve Bayes (NB) and Support Vector Machines (SVM) in document classification tasks, we decided on these two to be our primary classifiers of interest.

The project is broken into two phases for implementation, namely Phase 1 and Phase 2.

A. Phase 1

Phase 1 will be responsible for classifying cybersecurity courses into the five competency levels defined in the Cyber-CHAMP model. These competency levels are Novice, Fundamentals, Intermediate, Advanced, and Expert. In the Jung repository, course competency level was prelabeled and assigned to their respective courses, allowing us to skip manually labeling courses to their proper competency levels. In this approach, each row in the repository had its column data aggregated into one text paragraph, minus the value from the ‘Course Competency’ column. This data was then split into a tuple, with the first entry being the raw text and the second entry the value of the course competency.

In this approach, we vectorized the raw text into a Term Frequency – Inverse Document Frequency vector (TF-IDF) and applied the Multinomial Naïve Bayes (MultinomialNB) and Stochastic
Gradient Descent (SGD) classifiers provided by Python package Scikit-learn to our data. SGD is a simple and efficient approach to fit linear classifiers and regressors, which in our case is SVM.

B. Phase 2

Phase 2 will be responsible for attributing NICE work-roles to the courses through Cosine Similarity (Prabhakaran, 2020) and Euclidian Distance (D'Agostino, 2009). Due to the utilization of TF-IDF and vectors to represent a document’s text, we chose Cosine Similarity and Euclidian Distance as similarities between vectors that represent text, serving as a proxy for textual similarity. Cosine Similarity is a commonly used technique to match similar documents and its approach focuses on the maximum number of common words between documents. Euclidean Distance, which is the shortest distance between two points, is a measure used to neutralize inaccurate Cosine Similarity outputs that occur when the number of common words increase as the size of a document increases, regardless of the document topics. When plotted on a multi-dimensional space, where each dimension corresponds to a word in the document, the Cosine Similarity captures the orientation (the angle) of the documents and the Euclidean distance computes the magnitude (Prabhakaran, 2020).

In this approach, information about the NICE work-roles and their respective TKSs were compiled each into one ‘document’, one for each NIST work-role. The raw text is then cleaned and stored in a Python ‘list.’ For each document in the Python list, stop words such as ‘the’ and ‘a’ are removed and the subsequent text is then vectorized using the vectorizer from Scikit-learn into TF-IDF vectors. The same process is repeated for the training course data, and the similarity is calculated through ‘cosine_similarity’ and ‘euclidian_distances’ methods from Scikit-learn. The results are then stored within a similarity matrix, and the most relevant documents can then be retrieved.

V. Results and Discussion

A. Phase 1: Naïve Bayes (NB) & Support Vector Machines (SVM) Approach

1. Accuracy

Both classifiers are commonly used in text/document classification due to their relatively high accuracy, but it was somewhat surprising to see that both NB and SVM Classifiers hovering around 50% accuracy. To evaluate accuracy, we considered the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). Accuracy is calculated as:

\[
\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}
\]

The NB classifier had a 47.05% accuracy, and the SVM classifier had a 54.90% accuracy. Once we optimized the model hyperparameters with the GridSearch package from scikit-learn, we were able to achieve a 66.83% accuracy with NB, and an accuracy of 88.08% for SVM. For the NB
classifier, a classifier considered as one of the best document classifiers (Ting, Ip, & Tsang, 2011), it yielded surprisingly low accuracy even with optimized hyperparameters. Due to SVM having a higher accuracy compared to the NB classifier, we chose to proceed with SVM for the rest of our model.

2. Interpretation of Confusion Matrix

A confusion matrix is used to evaluate the quality of the output of a classifier on a dataset. High values along the diagonal indicate correct classification, and high values on the non-diagonal entries signal misclassification (the model’s predicted label is different from the true label). We can see this visually with the color of the tile, as darker colored tiles indicate a greater accuracy.

The intersection of a row and a column in a confusion matrix represents the percentage correctly classified between labels. In Figure 2 below, the intersection between the Fundamentals labels is at 31.37%. This shows that out of the predicted Fundamentals labels, 31.37% were the true label of Fundamentals.

In Figure 2, we can see the Naïve Bayes classifier is having trouble accurately classifying Intermediate, Expert, and Advanced labels, while it is able to classify Fundamentals and Novice labels with reasonable success. The NB classifier is having trouble distinguishing between the Novice and Intermediate labels and is classifying them as Fundamentals.
We can see in Figure 3 the SVM classifier is able to classify the Fundamentals label considerably well, and it is having trouble distinguishing between the pairing of Fundamentals & Novice and Fundamentals & Intermediate. Like the Naïve Bayes classifier, it is having a difficult time classifying Expert labels, having a 0% accuracy overall.

**B. Phase 2: Cosine Similarity & Euclidean Distance**

Due to time constraints and the nature of the dataset, accuracy metrics would most likely prove unhelpful in validating our model due to the sheer number of labels and the fact each course can have multiple NICE work-roles as labels.

An alternative approach to quantifying how well this model performed is outlined in the section for future work.

While we were not able to generate a quantifiable metric of how well our model performed, our model does seem to provide its intended functionality, as shown in the figure below.

In Figure 4, we can see the document is returning a list of NICE role abbreviations with Cosine Similarity serving as a proxy for how relevant the NICE role is to the course (Refer to Figure C1 for the full output). The example course description’s key phrase “…implementing and sustaining a cyber security [sic] program at a nuclear and/or radiological facility.”
In the NICE role descriptions spreadsheet, the role ‘ovmgt001’ returns the following description:

Information Systems Security Manager - Responsible for the cybersecurity of a program, organization, system, or enclave.

This seems to closely match the description of what skills the example course would like the user to learn.

Searching for the role with the lowest Cosine Similarity, ‘cocl002’, which had a Cosine Similarity of 9.06% (Not pictured in Figure 4, available in Figure C1), returned a position with the description of:

All Source-Collection Manager – Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

This position description does not seem to align with the course’s goals, which suggests our model is working correctly.

VI. Conclusions

Through the combination of Phase 1 and Phase 2 approaches, our model pipeline can receive general characteristics of a cybersecurity course, and successfully categorize the course into the proper competency level and return the associated NICE work-roles with Cosine Similarity serving as a proxy for percent match for relevancy. Our code has been modularized into a singular python script named ‘b_script.py’ and can be used within other tools to classify courses.

Figure 5 demonstrates how our script works. The script can receive a course’s description along with any other attributes of the course, and now can return a python dictionary with the competency level and the relevant NICE roles as output, all within one model (full output available in Figure C2).
While the results are preliminary due to a limited dataset, our approach shows document classification through NLP techniques such as SVM and NB is possible and should be further investigated as an alternative to the manual and subjective classification of training courses present in the industry today. Automation of course classification comes with many benefits. Automation reduces the need for manual labor, offers a more objective approach to classification, can deal with large amounts of data quickly, and offers a flexible solution that can be used by many industries regardless of unique workforce constraints—provided a standardization framework such as NICE exists within that industry.

VII. Future Work

Utilizing methods such as NB, SVM, Cosine Similarity, and Euclidean Distance, our approach yielded promising results. An alternative implementation geared towards optimizing the model and increasing the accuracy is to use new transformer-based architectures, namely Google’s Bidirectional Encoder Representations from Transformers (BERT), to generate context-based word embeddings, allowing the model to also consider locations of words within a sentence to see if this yields better results.

The logical next step for this project is to run the aggregated training course data through the script and build a repository of training courses with their predicted competency level as well as the
NICE roles with the percent similarity included. This will be the ‘indexable’ course catalog mentioned previously.

In the future, we intend to integrate our indexable course catalog with the Cyber-CHAMP Task Analysis Survey, allowing Cyber-CHAMP users to find courses that match their competency level as well as their work-role description. The Cyber-CHAMP Task Analysis Tool will assess a user’s competency and most relevant NICE role. The tool can then search based on those criteria, producing a list of relevant courses for the user using our indexable course catalog.

Another point of interest for future work is to determine a way to calculate the ‘cut-off’ point for relevancy. This is because, at a certain point, the NICE work-roles returned from our script begins to not accurately describe the input course at all.

As mentioned previously in the results section, a proposed approach to quantifying the performance of the Cosine Similarity and Euclidian Distance model is to use a weighted score for each course categorized and cross-referencing the predictions to the correct NICE roles on the ‘Work-Role to Training Map’ spreadsheet in Jung’s repository. Our original training dataset did not have the NICE roles labeled, so this alternative approach can address this issue.

Finally, we would also like to aggregate more training course data. For the majority of the project, we did not have access to enough clean data to effectively reach a conclusion, so the collection of more course data will further legitimize our results.

VIII. References

Argonne National Laboratory. (2020). Enterprise Wide Assessment of Courses: Analysis of FEMA’s State, Local, Tribal, and Territorial Training Courses. FEMA.


Jiawei Han, M. K. (2012). Getting to Know Your Data. In Data Mining (Third Edition) (pp. 39-82). Morgan Kaufmann.


THIS PAGE INTENTIONALLY LEFT BLANK
Appendix A – COSTAR Analysis and 5-Minute Brief

Customer: Who are the intended customers, and what are their important unmet needs?

We hope to serve any industry that has workforce development and training through courses in the cybersecurity space. Our tool will address the “Jack of all trades, master of none.” issue in the cybersecurity workforce where employees are in charge of many tasks that don’t particularly fall into the scope of their position. This reduces job specialization and employees’ task competency considerably.

Opportunity: What is the full size of the opportunity?

We have the potential to create the first tool to index training courses across the cybersecurity industry by work-role and competency level. This tool could also be extended to any industry with an existing standardized work-role framework.

Solution: What is your proposed solution for capturing the opportunity?

We are proposing an indexable course catalog of cybersecurity courses to NIST/NICE and ICS work-role mapping. We have compiled our code including our model into a singular Python script as we are working on implementation of a catalog that can be utilized as a tool. Our mode can be integrated the into Cyber-CHAMP’s Task Analysis Tool—giving employees more insightful results on their specific course needs than the current tool. We have also documented our code for readability and replication, keeping possible future improvement efforts in mind.

Team: Who needs to be on your team to ensure your solution’s success?

The team currently includes two juniors from Purdue University; Kevin Tian who is double majoring in Data Science and Applied Statistics, and Bengisu Cuneyit who is majoring in Computer Science and minoring in Mathematics, as well as our mentor Dr. Gary M. Deckard from INL.

Our team’s technical background was a big contributor in our impressive preliminary results and promising conclusions. We hope to continue this project throughout fall and spring if we can receive the needed funding. We would also like to add more interns to the team who have similar backgrounds in order to make the project larger in scale and streamline some of the work.

Advantage: What is your solution’s competitive advantage over alternatives?

<table>
<thead>
<tr>
<th>Current Industry Approach</th>
<th>Our Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗ Manual tagging of courses through Subject Matter Experts</td>
<td>✓ Automatic tagging of courses through Machine Learning</td>
</tr>
<tr>
<td>✗ Model is subjective and classification can differ between experts</td>
<td>✓ An objective approach to classifying courses</td>
</tr>
<tr>
<td>✗ Is not scalable for a large number of courses, will require large amount of manual labor</td>
<td>✓ Can handle large inputs of courses through our model pipeline</td>
</tr>
</tbody>
</table>
Some approaches can only be applied to a single industry due to initial work needed to set up  

Flexible and can apply to industries outside of the cybersecurity space (medical, business, etc.)

**Results:** What results will be achieved from your solutions?

By offering the correct courses to employees, we will try to encourage work-role awareness and increase specialization in the workforce by solving the previously mentioned ‘Jack of all trades…’ problem.

Our project is also a chance for INL to be recognized as the first organization to introduce such a tool into the cybersecurity space. This could get our names out as pioneers in the industry and create a good amount of positive exposure for the laboratory. INL’s eminence will also increase through the publication of an article on our project in an IEEE Research Journal.
Appendix B – Code Repository

Unless stated otherwise, the original format of the code are Jupyter Notebook style code blocks.

Demo Notebook for modularized code

```python
#!/usr/bin/env python
# coding: utf-8

# In[1]:
import b_script

# In[2]:
course = 'Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility. The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program. This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event.'

# ## Input
# "Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility. The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program. This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event."

# ## Output
# In[3]:
b_script.analyze(course)
```

Modularized Phase 1 and Phase 2 Code (Python Script)

```python
#!/usr/bin/env python
# coding: utf-8

# In[6]:
import pandas as pd
import numpy as np
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.feature_extraction.text import TfidfTransformer
from sklearn.linear_model import SGDClassifier
from sklearn.pipeline import Pipeline
```
import pickle
from sklearn.model_selection import GridSearchCV
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.metrics.pairwise import cosine_similarity
from sklearn.metrics.pairwise import euclidean_distances
import re

# In[7]:
def analyze(courseDesc):
    train = pd.read_csv('train.csv')
    test = pd.read_csv('test.csv')
    train = train.sample(frac=1)
    count_vect = CountVectorizer()
    X_train_counts = count_vect.fit_transform(train.data)
    tfidf_transformer = TfidfTransformer()
    X_train_tfidf = tfidf_transformer.fit_transform(X_train_counts)
    text_clf = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()), ('clf-svm',
        SGDClassifier(loss='perceptron', penalty='l2', alpha=1e-3, random_state=42)),])
    text_clf.fit(count_vect.fit_transform(train.data), train.target)
    predicted_svm = text_clf.predict(test.data)
    # np.mean(predicted_svm == test.target)
    parameters_svm = {'vect__ngram_range': [(1, 1), (1, 2)], 'tfidf__use_idf': (True, False), 'clf-svm__alpha': (1e-2, 1e-3),}
    gs_clf_svm = GridSearchCV(text_clf, parameters_svm, n_jobs=-1)
    gs_clf_svm = gs_clf_svm.fit(train.data, train.target)
    testdf = pd.DataFrame({'data': [courseDesc],})
    testdf.columns = ['data']
    count_vect = CountVectorizer()
    inf = count_vect.fit_transform(testdf.data)
    shp = list(inf.shape)
    outDict = {};
    outDict['compLevel'] = compLevel
    ## Cosine Similarity
    new = pd.read_csv('cleaned_nice_ksas.csv')
    coursedf = pd.DataFrame([courseDesc])
    coursedf.columns = ['descriptions']
    new = coursedf.append(new)
    tfidfVectoriser = TfidfVectorizer()
    tfidfVectoriser.fit(new.descriptions)
    tfidf_vectors = tfidfVectoriser.transform(new.descriptions)
    pairwise_similarities = np.dot(tfidf_vectors.tfidf_vectors.T).toarray()
Cleaning Jung dataset for course to NICE Work-role mapping

```python
import pandas as pd
import numpy as np
import re
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.feature_extraction.text import TfidfTransformer
from nltk.corpus import stopwords
from nltk.tokenize import word_tokenize
```
In[159]:
data = pd.read_csv('jungdsfull.csv')

In[160]:
data = data.drop(['Classified'], axis = 1)

In[161]:
data.fillna('No', inplace = True)

In[162]:
data = data.drop(['Link', 'Learning Path', 'Learning Path Name'], axis = 1)

In[163]:
data = data.applymap(lambda x: x.lower())

In[164]:
data = data.applymap(lambda x: x.translate(str.maketrans('', '', string.punctuation)))

In[165]:
data = data.applymap(lambda x: ' '.join(x.split()))

# Assembly into one document & saving to CSV, only needs to be run once

# documents = []

# ]

# ]

# ]

# ]

# ]

# ]

# ]

# ]

# ]

# ]
Handling Cyber-CHAMP Dataset, Jung Dataset, and implementation of Naïve Bayes & SVM Classifiers:

```python
#!/usr/bin/env python
# coding: utf-8

# In[49]:
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.feature_extraction.text import CountVectorizer

# In[50]:
data = pd.read_excel(io = "jung.xlsx", sheet_name = "Trainings", engine='openpyxl')
```

```python
# In[51]:
```
data.shape

# In[52]:

data.columns

# In[53]:

print(data['Competency Level'].count())
print(data['Competency Level'].isna().sum())

# In[54]:

data = data[data['Competency Level'].notna()]

# In[55]:

counts = data['Competency Level'].value_counts().to_list()
print(data['Competency Level'].value_counts())

cat = tuple(data['Competency Level'].value_counts().index.to_list())

# In[56]:

for i in dlist:
    comp = i[11]
    i.pop(11)
    string = " ".join(str(x) for x in i)

# In[57]:

fig, ax = plt.subplots()
ax.bar(cat, counts)
fig.autofmt_xdate()
plt.show()

# In[58]:

proc_entries = []
string = " " :join(x for x in (list(string.replace('nan', '').split())))

proc_entries.append((string, comp))

# In[11]

proc_entries[-1] = (proc_entries[-1][0], 'Expert')
proc_entries[-2] = (proc_entries[-2][0], 'Expert')

# In[60]:

# In[61]:

# In[62]:

adj_cat = list(cat)
adj_cat.pop(5)
counts.pop(5)
counts[4] = 11

# In[63]:

# In[64]:

# In[65]:

data = open("CyberCHAMP.txt", "r")
rawtext = data.read()
courses = re.split("(?<!S)\d+(?!C)\", rawtext)

# In[66]:

my_list = []

for course in courses:
    fixed_course = course.replace("\", "")
    fixed_course = fixed_course.replace("\", "")
    fixed_course = fixed_course.replace("\", "")
    fixed_course = fixed_course.replace("\", "")
fixed_course = fixed_course.split()

fixed_course = " ".join(fixed_course)

my_list.append(fixed_course)

157. # In[67]:
158.
159.
160. for i in my_list:
161.  print(i + \\
162. 163.
164. # In[68]:
165.
166.
167. competency = [i.split() for i in my_list]
168. competency.remove("ICS")
169. print(competency)
170.
171.
172. # In[69]:
173.
174.
175. new_list = [i.split(', 1) for i in my_list]
176. for x in new_list:
177.  print(x)
178.
179.
180. # In[70]:
181.
182.
183. for i in new_list:
184.  if i[0] == 'Design':
185.   i[0] = 'Expert'
186.
187.
188. # In[71]:
189.
190.
191. astuple = []
192. for i in new_list:
193.   astuple.append((i[1], i[0]))
194.
195. astuple.pop(0)
196.
197.
198. # In[72]:
199.
200.
201. test = pd.DataFrame(astuple)
202.
203.
204. # In[73]:
205.
206.
207. #test.loc[1][‘data’]
208.
209.
210. # In[74]:
211.
212.
213. test
214.
215.
216. # ### Naive Bayes
217.
# In[75]:

218. train = pd.DataFrame(proc_entries)

219. train.columns = ['data', 'target']  
220. train = train.sample(frac = 1)  
221. # Shuffle dataframe

222. # In[76]:

223. from sklearn.feature_extraction.text import TfidfTransformer

224. tfidf_transformer = TfidfTransformer()

225. X_train_tfidf = tfidf_transformer.fit_transform(X_train_counts)

226. # In[77]:

227. from sklearn.naive_bayes import MultinomialNB

228. clf = MultinomialNB().fit(X_train_tfidf, train.target)

229. # In[78]:

230. from sklearn.pipeline import Pipeline

231. text_clf = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()), ('clf', MultinomialNB())])

232. text_clf = text_clf.fit(train.data, train.target)

233. # In[79]:

234. test.columns = ['data', 'target']

235. test = test.sample(frac = 1)

236. predicted = text_clf.predict(test.data)

237. rslts = {'(Before) Naive Bayes': np.mean(predicted == test.target)}

238. # In[80]:

239. # SVM

240. # In[81]:

241. # In[82]:

242. # In[83]:
from sklearn.linear_model import SGDClassifier

text_clf_svm = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()), ('clf-svm', SGDClassifier(loss='perceptron', penalty='l2', alpha=1e-3, random_state=42))])

_ = text_clf_svm.fit(train.data, train.target)
predicted_svm = text_clf_svm.predict(test.data)
np.mean(predicted_svm == test.target)

rslts['(Before) SVM'] = np.mean(predicted_svm == test.target)

# ### Using Gridsearch (SVM)

parameters_svm = {'vect_ngram_range': [(1,1), (1,2)], 'tfidf_use_idf': [True, False], 'clf-svm_alpha': [1e-2, 1e-3],}

gs_clf_svm = GridSearchCV(text_clf_svm, parameters_svm, n_jobs=-1)
gs_clf_svm = gs_clf_svm.fit(train.data, train.target)
print(gs_clf_svm.best_score_)
print(gs_clf_svm.best_params_)

rslts['(Best Score) SVM'] = gs_clf_svm.best_score_

# ## Saving SVM Model

# 1st method

dump(gs_clf_svm, 'gs_clf_svm.joblib')

clf = load('gs_clf_svm.joblib')
import pickle

pickle.dump(gs_clf_svm, open('clf_model.sav', 'wb'))

clf = pickle.load(open('clf_model.sav', 'rb'))

parameters = {'vect__ngram_range': [(1, 1), (1, 2)], 'tfidf__use_idf': [True, False], 'clf__alpha': (1e-2, 1e-3),}

gs_clf = GridSearchCV(text_clf, parameters, n_jobs=-1)
gs_clf.fit(train.data, train.target)
print(gs_clf.best_score_)
print(gs_clf.best_params_)

rslts['(Best Score) Naive Bayes'] = gs_clf.best_score_

# ### Results

from sklearn import metrics

print(rslts)

#print(metrics.classification_report(test.target, pred_gs_svm))
```python
415. svm_matrix = metrics.confusion_matrix(test.target, predicted_svm)
416. nb_matrix = metrics.confusion_matrix(test.target, predicted)
417.
418. # ### Inference
419.
420. # In[ ]:
421.
422.
423.
424. testdf = pd.DataFrame(['Remember FG07- Intro to Industrial Processes, Measurement and Control ISA $3,855 Live; 4.5 days 3.2 CEU’s This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.', 'Design', 'Maintain', 'Remember'],)

425.
426.
427. # In[ ]:
428.
429.
430. testdf.columns = ['data']
431.
432.
433. # In[ ]:
434.
435.
436. count_vect = CountVectorizer()
437. inf = count_vect.fit_transform(testdf.data)
438. shp = list(inf.shape)
439.
440.
441. #
442. #
443. # <em><strong>‘Remember FG07- Intro to Industrial Processes, Measurement and Control ISA $3,855 Live; 4.5 days 3.2 CEU’s This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.’</em></strong></em>
444. #
445. #
446. # Should return 'Fundamentals'
447. # In[ ]:
448.
449. list(text_clf_svm.predict(testdf.data))[0]
450.
451. #
452. # <em><strong>‘Design’</em></strong></em>
456. # Should return 'Expert'
461. # In[ ]:
462.
463. list(text_clf_svm.predict(testdf.data))[1]
466.
469. #
470. #
471. #
472. # Should return 'Maintain'
```

CURRICULUM ANALYSIS THROUGH MACHINE LEARNING
list(text_clf_svm.predict(testdf.data))[2]

# In[ ]:

list(text_clf_svm.predict(testdf.data))[3]

# In[ ]:

import seaborn as sns

target_names = list(text_clf_svm.classes_)

fig, ax = plt.subplots()
sns.heatmap(svm_matrix/np.sum(svm_matrix), fmt='.2%', cmap='Blues', annot=True, ax=ax, square=False)

ax.set_xlabel('Predicted Labels', fontsize=20)
ax.set_ylabel('True Labels', fontsize=20)
ax.set_title('Confusion Matrix (SVM)', pad=20)
ax.xaxis.set_ticklabels(target_names)
ax.yaxis.set_ticklabels(target_names)
fig.autofmt_xdate()
plt.yticks(rotation=360)
plt.show()
Cleaning Cyber-CHAMP Dataset

```python
def cleaning(text):
    courses = re.split("(?<!\S)\d|(?!C)", rawtext)
    my_list = []
    for course in courses:
        fixed_course = course.replace("\", " ").split()[:-1]
        fixed_course = " ".join(fixed_course)
        my_list.append(fixed_course)
    competency = [i.split()[:-1] for i in my_list]
    competency.remove("ICS")
    print(competency)
    new_list = [i.split()[:-1] for i in my_list]
    for x in new_list:
        print(x)
    for i in new_list:
        if i[0] == 'Design':
            i[0] = 'Expert'
        astuple = []
        astuple.append((i[1], i[0]))
        astuple[1:] =
    print(astuple)
```

NIST NICE Work-role cleaning

```python
def nist_cleaning(text):
    def nist_cleaning(text):
        courses = re.split("(?<!\S)\d|(?!C)", rawtext)
        my_list = []
        for course in courses:
            fixed_course = course.replace("\", " ").split()[:-1]
            fixed_course = " ".join(fixed_course)
            my_list.append(fixed_course)
        competency = [i.split()[:-1] for i in my_list]
        competency.remove("ICS")
        print(competency)
        new_list = [i.split()[:-1] for i in my_list]
        for x in new_list:
            print(x)
        for i in new_list:
            if i[0] == 'Design':
                i[0] = 'Expert'
            astuple = []
            astuple.append((i[1], i[0]))
            astuple[1:] =
        print(astuple)
```
# In[]:

## Preprocessing

```
# In[39]:
df = pd.read_csv("tasks.csv")
```

```
# In[40]:
df = df.transpose().reset_index()
```

```
# In[41]:
df.columns = list(df.loc[0])
```

```
# In[42]:
df = df.drop(0)
```

```
# In[43]:
df2 = pd.read_csv('role2task.csv')
```

```
# In[44]:
df2.head()
```

## Course Dataset

```
# In[45]:
courses = pd.read_csv('course dataset.csv')
```

```
# In[46]:
courses.columns = ['entries']
```

```
# In[47]:
courseList = list(courses.entries)
```

```
# In[48]:
```
courseList

# ## Text cleaning conversion to dictionary format

# In[49]:
adjList = []

# In[50]:

## So the last entry in courseList is the "]" so its not actually an entry
for a in range(0,len(courseList)-1):
  print(a)
  mt = re.search('[^,]', courseList[a])
  temp = courseList[a].replace(mt.group(), '')
  temp = temp.replace("relatedRoleIds": "", ""
  temp = temp.replace("false", "False")
  temp = temp.replace("true", "True")
  temp = temp.replace("None")
  roles = mt.group()
  roles = roles.replace("", "")
  roles = roles.replace("V", "")
  roles = roles.replace("T", "")
  roles = roles.replace("", "")
  y=json.loads(temp)
  y['roles'] = roles.split(""
  adjList.append(y)

# In[51]:

adjList[3]

# In[52]:

pd.DataFrame(adjList)

# ## Creating Role dictionary

# In[53]:
roles = pd.read_csv('role2task.csv')

# In[54]:
workRoles = list(roles['Work Role ID'])

# In[55]:

CURRICULUM ANALYSIS THROUGH MACHINE LEARNING
for i in range(0, len(workRoles)):
    workRoles[i] = workRoles[i].strip()

# In[56]:

workRoles

# In[57]:
categories=workRoles.copy()
workRoles.insert(0, 'text')

# In[58]:

workRoles

# In[59]:

tempDict = {}

for i in workRoles:
    tempDict[i] = [0]

pd.DataFrame.from_dict(tempDict)

# In[60]:

def cleantxt(text):
    return text

# In[61]:
p = []

for i in adjList:
    currentRoles = i['roles']
    txt = ''
i.pop('AdvTrURL', None)
    for x in i.keys():
        if x is not 'roles':
            txt = txt + i[x] + ' '

    temp2= tempDict.copy()  
    for j in currentRoles:
        temp2[j] = [1]
    txt = txt.split()
    temp2['text'] = " ".join(txt)
    p.append(temp2)

# In[62]:

CURRICULUM ANALYSIS THROUGH MACHINE LEARNING
tempDF = pd.DataFrame()
for i in p:
    tempDF = tempDF.append(pd.DataFrame(i))

tempDF = tempDF.reset_index().drop(['index'], axis=1)

# ## Saves the data as CSV

# In[76]:

#tempDF.to_csv('fixed_data.csv')

# In[64]:

# In[64]:

Using the ISA/IEC 62443 Standards to Secure Your Control Systems
The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition systems (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have worked so well on corporate information systems. This course provides a look at how the ISA/IEC 62443 standards can be used to protect your critical control systems. It also explores the procedural and technical difference between the security for traditional IT environments and those appropriate for SCADA or plant floor environments.

| $1,440 - $1800 | Online | Instructor-Assisted | Online | Intermediate | Novice |

Using the ISA/IEC 62443 Standards to Secure Your Control Systems
The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition systems (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have worked so well on corporate information systems. This course provides a look at how the ISA/IEC 62443 standards can be used to protect your critical control systems. It also explores the procedural and technical difference between the security for traditional IT environments and those appropriate for SCADA or plant floor environments.

| $1,440 - $1800 | Self-Paced | Online | Intermediate | Novice |

Assessing the Cybersecurity of New or Existing ICS Systems
The first phase in the ISA/IEC Cybersecurity Lifecycle Manifesto is to identify and assess ICS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. For ISA 62443-3 these assessments need to be performed as both new (i.e., greenfield) and existing (i.e., brownfield) applications. Part of the assessment process involves developing asset and conduct audits of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing ICS and to develop cybersecurity requirements specifications that can be used to document the cybersecurity requirements for the project.

| $1,800 | Self-Paced | Online | Intermediate | Novice |

Assessing the Cybersecurity of New or Existing ICS Systems
The first phase in the ISA/IEC Cybersecurity Lifecycle Manifesto is to identify and assess ICS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. For ISA 62443-3 these assessments need to be performed as both new (i.e., greenfield) and existing (i.e., brownfield) applications. Part of the assessment process involves developing asset and conduct audits of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing ICS and to develop cybersecurity requirements specifications that can be used to document the cybersecurity requirements for the project.

| $1,800 | Self-Paced | Online | Intermediate | Novice |

Assessing the Cybersecurity of New or Existing ICS Systems
The first phase in the ISA/IEC Cybersecurity Lifecycle Manifesto is to identify and assess ICS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. For ISA 62443-3 these assessments need to be performed as both new (i.e., greenfield) and existing (i.e., brownfield) applications. Part of the assessment process involves developing asset and conduct audits of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing ICS and to develop cybersecurity requirements specifications that can be used to document the cybersecurity requirements for the project.

| $1,800 | Self-Paced | Online | Intermediate | Novice |

Cythonology by Design: Implementation & Testing
Focuses on the selection associated with the design and implementation of ICS cybersecurity countermeasures. This involves the selection of appropriate cybersecurity controls based on risk and availability, the nature of the threats and vulnerabilities identified in the assess phase. This phase also includes cybersecurity exercises testing of the selected controls, in order to validate countermeasures are properly implemented and that the ICS has achieved the target security level. This course will provide students with the information and skills to implement and perform cybersecurity homework for the course or existing ICS in order to achieve the target security level assigned to each ICS based course or add. Additionally, students will learn how to develop and use a test plan to verify to that the ICS has achieved the target security level.

| 1 hour Free | Online | Online | Fundamentals |

Cythonology by Design: Implementation & Testing
Focuses on the selection associated with the design and implementation of ICS cybersecurity countermeasures. This involves the selection of appropriate cybersecurity controls based on risk and availability, the nature of the threats and vulnerabilities identified in the assess phase. This phase also includes cybersecurity exercises testing of the selected controls, in order to validate countermeasures are properly implemented and that the ICS has achieved the target security level. This course will provide students with the information and skills to implement and perform cybersecurity homework for the course or existing ICS in order to achieve the target security level assigned to each ICS based course or add. Additionally, students will learn how to develop and use a test plan to verify to that the ICS has achieved the target security level.

| 1 hour Free | Online | Online | Fundamentals |

Overview of IACS 62443 for Product Suppliers
The use of commercial of the shelf (COTS) technologies and the increase in interaction of industrial automation and control systems (IACS) has required IACS to consider vulnerabilities on information systems. The product supplier has a key role to play in the supply chain and the security of IACS solution.

| 36 hours | 900-985 | Online | Self-Paced | Intermediate |

Certified Automation Professional (CAP) Online Exam Review Course
This self-paced online course reviews the knowledge that is contained on the Certified Automation Professional (CAP) certification program examination. It is designed to prepare automation professionals who meet the exam criteria to take the exam. The content is based on the ISA/IEC 62443-3-2 Learning System preparation tool, as it incorporates content similarly included in that tool.

| 4 weeks | $1,640 - $2,000 | Online | Self-Paced | Intermediate |

Certified Automation Professional (CAP) Online Exam Review Course
This self-paced online course reviews the knowledge that is contained on the Certified Automation Professional (CAP) certification program examination. It is designed to prepare automation professionals who meet the exam criteria to take the exam. The content is based on the ISA/IEC 62443-3-2 Learning System preparation tool, as it incorporates content similarly included in that tool.

| 4 weeks | $1,640 - $2,000 | Online | Self-Paced | Intermediate |

Safety Instrumented Systems: A Life-Cycle Approach
The course focuses on the engineering requirements for safety specification, design, analysis, and justification of safety instrumented systems for the process industries. Students will learn how to determine safety integrity levels and evaluate whether proposed process systems meet the performance requirements.

| 3 weeks | $1,680 - $2,000 | Online | Self-Paced | Intermediate |

Fire and Gas System Engineering- Performance Based Methods for Process Facilities
This course will provide students with the information and skills to perform types of performance based designs (i.e., scenarios with accident production facility).

| 4 days | $1,300 - $1,595 | Online | Instructor-Assisted | Online | Fundamental |

Cybersecurity Practices for Industrial Control Systems
This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information in an enterprise may use as evidence. The training proceeds to teach mitigation possibilities in existing data systems, as well as other techniques to address those vulnerabilities.

| 3 hours Free | Online | Online | Fundamental |

Difference in Deployments of Industrial Control Systems
This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information in an enterprise may use as evidence. The training proceeds to teach mitigation possibilities in existing data systems, as well as other techniques to address those vulnerabilities.

| 3 hours Free | Online | Online | Fundamental |

Influence of ICS on Industrial Control Systems (ICIS)
If you understand what the components of IT networks do and how they communicate, you can better situation. Systems depend on technology that was not designed to protect our systems against the types of vulnerabilities in computer systems that run critical infrastructures. We have made effective techniques to address those weaknesses.

| 1 hour Free | Online | Online | Fundamental |

Influence of ICS on Industrial Control Systems (ICIS)
If you understand what the components of IT networks do and how they communicate, you can better situation. Systems depend on technology that was not designed to protect our systems against the types of vulnerabilities in computer systems that run critical infrastructures. We have made effective techniques to address those weaknesses.

| 1 hour Free | Online | Online | Fundamental |

Using the ISA/IEC 62443 Standards to Secure Your Control Systems
The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition systems (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have worked so well on corporate information systems. This course provides a look at how the ISA/IEC 62443 standards can be used to protect your critical control systems. It also explores the procedural and technical difference between the security for traditional IT environments and those appropriate for SCADA or plant floor environments.

| $1,440 - $1800 | Online | Instructor-Assisted | Online | Intermediate | Novice |
### Common ICS Components
This course covers the common components found in Industrial Control Systems (ICS). It reviews the components found in most ICS.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### Cybersecurity Within IT and ICS Domains
A move to integrate the components of Information Technology (IT) and Industrial Control Systems (ICS) has created security concerns, as interconnections between IT and ICS may increase the vulnerability of the ICS to cyber attacks. Understanding the basic concepts of cybersecurity will provide the necessary foundation to determine the appropriate controls to protect ICS. ICS are dependent on IT, as contemporary IT is often troubleshooted with cyber vulnerabilities.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### ICS Cybersecurity Risk
This course is designed to help you gain a better understanding of cyber risk. How it is defined in the context of ICS security, and the factors that contribute to it. This will empower you to develop cybersecurity strategies that align directly with the ICS environment. You will also learn how IT-based countermeasures can be customized to accommodate for the uniqueness of ICS architectures.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### ICS Cybersecurity Threats
Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect control systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### ICS Cybersecurity Vulnerabilities
In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and associated countermeasures that can be used to protect control systems.

- **Duration:** 2 hours
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### ICS Cybersecurity Consequences
Consider the potential impact of a successful cyber attack on your ICS. We usually assume that they will be more severe if you are manufacturing toxic chemicals that if you making simple widgets. A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you better understand the impacts of cyber-based attacks and provide you with different ways of looking at the potential consequences of three types of cyber threats.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### Attack Methodologies in IT & ICS
A good defense understands what the offense can do. So, the better you can think like an adversary, the better defenses or security you can set up that are specific to your system. Understanding how hacking attack systems helps you better understand how to defend against cyber attacks.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### Mapping IT Defense-In-Depth Security Solutions to ICS - Part I
This training will introduce the defense-in-depth model and cover layers 1 and 2.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### Mapping IT Defense-In-Depth Security Solutions to ICS - Part II
In the previous training, Mapping IT Defense-In-Depth Security Solutions to ICS - Part I, we covered layers 1 and 2 of the defense-in-depth model. In this module, we will pick up at layer 3: Network Security, and continue to build on the defense-in-depth strategy introduced in Part I.

- **Duration:** 1 hour
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### Introduction to Control Systems Cybersecurity
This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of compromise, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.

- **Duration:** 1 day
- **Cost:** Free
- **Level:** Varies
- **Format:** Fundamentals

### Intermediate Cybersecurity for Industrial Control Systems Part 1
This course builds on the concepts learned in the Introduction to ICS Cybersecurity (101) course. This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. In addition, this course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202), which often hands-on application of concepts presented.

- **Duration:** 1 day
- **Cost:** Free
- **Level:** Varies
- **Format:** Fundamentals

### Intermediate Cybersecurity for Industrial Control Systems Part 2
This course provides a brief review of Industrial Control Systems security. This includes a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample Process Control network that demonstrates exploitable use of unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises that will help the students develop Control Systems cybersecurity skills they can apply in their work environment.

- **Duration:** 1 day
- **Cost:** Free
- **Level:** Varies
- **Format:** Fundamentals

### ICS Cybersecurity
This course provides an online virtual training based on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks. In order to understand how to defend IT and OT systems, trainees will learn about common cyber vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of systems will enable trainees to identify mitigation strategies, policies, and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.

- **Duration:** 3 days
- **Cost:** Free
- **Format:** Online, Online
- **Level:** Fundamentals

### ICS Cybersecurity
This course is the companion and follow-on course to the 301V. This course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will follow a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity awareness and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture. This course is also intended to increase awareness of how a threat related to the Industrial Control System translates into a threat to business operations, either directly through the ICS or indirectly via network connections. Attendees will come to more fully appreciate that most businesses have numerous support processes and systems controlled by, or otherwise dependent on, an Industrial Control System.

- **Duration:** 5 days
- **Cost:** Free
- **Format:** Live, Online, Online
- **Level:** Novice
AC Variable Frequency drives have become very popular in recent years and have become an integral part of implementing Industrial Automation systems. This easy-to-launch course will help you understand everything about VFDs in a few hours.

HAZID

HAZOP

Fieldbus

Radiation Area Instrumentation

Gas Monitors

Radio-Frequency Identification (RFID)

AC Variable-Frequency Drives

Safe Chemical Warehousing

Industrial Cybersecurity

Most modern plants and facilities today use some kind of DCS, PLC, SCADA or SIS to monitor, control and safely shutdown the process. However, most of these Industrial Automation systems are not secure. This is why today DCS Security (also referred to as Industrial Cybersecurity) has become very important. In case of business and IT systems, a cybersecurity breach can result in monetary losses or loss of proprietary data. However in case of an Industrial cybersecurity incident, there can be a physical disaster since these cyber-physical systems control large plants and facilities that often time process huge amounts of hazardous, explosive and/or toxic materials.
Confined Space Safety

Confined Space Safety Training & Certification - compliant with OSHA guidelines
A Lack Of Knowledge Can Cost You Jobs, Your Money, Your Business... Even Your Life. Shocking Fact: Every year hundreds of employees die every year and thousands from ignorance about working in confined spaces. The employees lose their jobs, their best workers.

3 hours $395 - $599 Online - Online - Fundamentals

Hazardous Area Classification

This course was designed and is taught by two highly experienced professionals. A former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

Industrial Toxicology

Toxicology is the study of poisons. Many industrial processes use materials that are either toxic by themselves or create materials that may be toxic by-products. These toxins may affect humans, plants, animals and the environment. This course is in the popular Advisor NERSC format. This means that you will see a mix of lectures, animations, videos and pictures, real-life examples and exercises that help you gain a deep understanding of the subject.

ICS Cybersecurity for Managers

This course was developed and is taught by two highly experined professionals: a former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

ICS Cybersecurity in Depth

This course is designed and is taught by two highly experienced professionals. A former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

ICS/SCADA Security Essentials

This course was developed and is taught by two highly experienced professionals: a former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

ICS Active Defense and Incident Response

This course was developed and is taught by two highly experienced professionals: a former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

Ansewering and Exploiting Control Systems

This course is designed and is taught by two highly experienced professionals: a former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

Certified SCADA Security Architect (CSSA)

This course is designed and is taught by two highly experienced professionals: a former CEO of an oil and gas company and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a “Reader’s Digest” of what the instructors have learned over the last decade regarding effective risk assessment and implementation of an OSHA compliance program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company’s OSHA compliance program.

ICS/SCADA Cyber Range: Get Out or Capture the Flag

Put your white hat on and try to prevent a major disaster from happening by using ICS/SCADA pentesting challenges.

40 minutes $49/month - $59/month - On-Demand - Anywhere - Intermediate - Advanced

ICS/SCADA Cyber Range: Get Out or Capture the Flag

Put your white hat on and try to prevent a major disaster from happening by using ICS/SCADA pentesting challenges.

40 minutes $49/month - On-Demand - Anywhere - Intermediate - Advanced

SCADA Security Frameworks

This course will begin your introduction to SCADA security frameworks, covering common themes to SCADA, relevant security standards and models, developing SCADA security policies and more.

40 minutes $49/month - On-Demand - Anywhere - Intermediate

SCADA Security Assessment

Review your understanding of SCADA security assessment with this course covering SCADA security objectives, security assessment programs and more.

40 minutes $49/month - On-Demand - Anywhere - Intermediate

SCADA Device Identification and Analysis

Make sure you know what you need to know with this course on SCADA device identification and analysis.

40 minutes $49/month - On-Demand - Anywhere - Intermediate

CURRICULUM ANALYSIS THROUGH MACHINE LEARNING

39
SCADA Vulnerabilities
Explore SCADA vulnerabilities with this course covering common vulnerabilities, vulnerability scanning, server obfuscation and more.
36 minutes
$34/month
On-Demand
Anywhere
Intermediate

Penetrating SCADA Services and Protocols
Review what it takes to attack standard services, server OS, ES protocols and more with this course on penetrating SCADA services and protocols.
36 minutes
$34/month
On-Demand
Anywhere
Intermediate

SCADA Access Controls
In this course, you'll look at the importance of SCADA access controls. Review physical safety, access control models and more.
36 minutes
$34/month
On-Demand
Anywhere
Novice

Remote Access and Hostile Security
Be familiarize yourself with the challenges of remote access technologies, field site forewards and more.
36 minutes
$34/month
On-Demand
Anywhere
Novice

SCADA Network Security
In this course, you'll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security issues.
36 minutes
$34/month
On-Demand
Anywhere
Advanced

SCADA Intrusion Detection and Incident Response
Set to gain what you need to know for SCADA intrusion detection and incident response.
36 minutes
$34/month
On-Demand
Anywhere
Novice

SCADA Penetration Testing
Brush up on what you need to know to conduct security checks on this course on SCADA penetration testing.
36 minutes
$34/month
On-Demand
Anywhere
Novice

Advanced Insider Threats Threading
The purpose of this course is to highlight capabilities in the frameworks that mitigate risk posed by insider threats.
36 minutes
$34/month
On-Demand
Anywhere
Fundamentals

Consequence-driven Cyber-informed Engineering (CDCE)
Consequence-driven Cyber-informed Engineering (CDCE) is a new methodology focused on ensuring the nation’s critical infrastructure systems. Developed at Battelle National Laboratory, CDCE has the assumption that if a critical infrastructure system is targeted by a concerted and determined adversary, the targeted network can and will be penetrated. This methodology forverts to the core concept of managing the consequences of a cyber security program. This includes identifying sources of risk, potential of digital systems, detection concepts and protection led, response to detection points, and protecting the system back to conditions before a cyber event.
3 days
In Person
Fundamentals

Cyberstrike
In this course, you’ll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security issues.
2 days
$34/month
On-Demand
Anywhere
Fundamentals

Maritime ICS Cybersecurity Fundamentals
This course will provide participants with knowledge of maritime control systems, general concepts of cyber-security and maritime cyber threats. The course provides an understanding of maritime cyber threat and response measures through the development, testing and implementation of tactics, techniques, and procedures.
2 days
In Person
Fundamentals

Managing Cyber Risks
This course is an introductory course that covers awareness of cyber risks to potential vulnerabilities in nuclear facilities. The course provides important concepts and awareness training to participants.
10 days
Advanced

SCADA Preventative Controls
This two-day course will provide participants with a baseline of knowledge and skills regarding SCADA preventative controls.
16 hours
$34/month
On-Demand
Anywhere
Novice

Cybersecurity Fundamentals
This is a high level intro course designed to expose participants to the challenges and frameworks used in implementing and maintaining a cyber security program in nuclear and/or industrial facility. The course uses the National Institute of Standards and Technology (NIST) cybersecurity framework for the course structure for covering the core concepts and components of cyber security programs. It includes identifying sources of risk, potential of digital systems, detection concepts and protection led, response to detection points, and protecting the system back to conditions before a cyber event.
3 days
In Person
Fundamentals

Cybersecurity Assessment
This two-day training is designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting industrial control systems. This training offers participants a hands-on, real-world demonstration of a cyberattack, drawing from elements of the 2013 Stuxnet/0day incident. During this training participants are guided through a series of in-depth challenges/owners to defend against understand the equipment they individually encounter within their industrial environments.
10 days
Advanced

DOD/DOJ Radiography Techniques Training (ARDT)
This training provides members of the US WMD-CST advanced concepts for use in response to an RDD detonation. The course is designed to be a follow-on training to Cyberstrike and provides detailed instruction and practice on the procedures and techniques used to recover radioactive sources and provide radiological site assessments of areas suspected to be contaminated with radiological materials. The course also provides an overview of the roles and responsibilities of Cyberstrike participants and the Cyberstrike course structure for conveying the core concepts and components of cyber security to participants.
20 days
Novice

DHS Basic Incident Responder Training (BIRT)
This training provides members of the US WMD-CST advanced concepts for use in response to an RDD detonation. The course is designed to be a follow-on training to Cyberstrike and provides detailed instruction and practice on the procedures and techniques used to recover radioactive sources and provide radiological site assessments of areas suspected to be contaminated with radiological materials. The course also provides an overview of the roles and responsibilities of Cyberstrike participants and the Cyberstrike course structure for conveying the core concepts and components of cyber security to participants.
20 days
Novice

IAEA Computer Security for Nuclear Facilities
The purpose of this 2 week training is to educate participants regarding computer security related issues within nuclear security of nuclear facilities. The training provides participants with key technologies found in nuclear facilities, identify risks involved in accessing cyber risk and cyber security and provide a framework for the workshop with a greater understanding of the digital footprint through cyber risk. The training, how to access those vulnerabilities, and how to protect against those vulnerabilities.
20 days
Advanced

Maritime Nuclear Criticality Safetylesen (CCE ACCElerate) Engineering (CCE)
This training will provide participants with knowledge of the core concepts and skills specific to critical infrastructure elements, including industrial control systems (ICS) and their cyber components on maritime platforms. Specifically, this course covers the industry platforms, systems of systems, understanding information technology (IT) and controls, and feedback-control system concepts. Most importantly, it will highlight the cyber interdependencies of each system on another.
16 hours
Advanced

Advanced Radiation Detection Training (ARDT)
This training is for the National Radiological (NRR) Civil Support Team personnel, providing hands-on training on detection of sources, DRG training, dosimeters, personnel- and equipment-based measurements. The course provides learning, training, and demonstration exercises, both in class and offsite locations.
Advanced

Advanced Radiological Detection Training (ARDT) WMD Civil Support Team (RHOC)
This training is for the National Radiological (NRR) Civil Support Team personnel, providing hands-on training on detection of sources, DRG training, dosimeters, personnel- and equipment-based measurements. The training enables members of the WMD-CST team to identify hazards, assess consequences, and advise on response measures through the development, testing and implementation of tactics, techniques, and procedures.
Advanced

DOD/DOJ Radiography Techniques Training (ARDT)
This training is for the National Radiological (NRR) Civil Support Team personnel, providing hands-on training on detection of sources, DRG training, dosimeters, personnel- and equipment-based measurements. The training enables members of the WMD-CST team to identify hazards, assess consequences, and advise on response measures through the development, testing and implementation of tactics, techniques, and procedures.
Advanced

NNSA Mark 28 Photography Techniques Training (RHOC)
This training, conducted by DOD WMD through RHOC, provides the highest-fidelity overview of nuclear photography training for the Federal Radiological (RHOC) Radiographers. The National Laboratories provide special technical support by providing technical support for training technical exercises, exercises, both in class and offsite locations.
Advanced

NNSA Mark 28 Photography Techniques Training (RHOC)
This training, conducted by DOD WMD through RHOC, provides the highest-fidelity overview of nuclear photography training for the Federal Radiological (RHOC) Radiographers. The National Laboratories provide special technical support by providing technical support for training technical exercises, exercises, both in class and offsite locations.
Advanced

Nuclear Explosions Detection (DOD)
This training, conducted by DOD WMD through RHOC, provides the highest-fidelity overview of nuclear photography training for the Federal Radiological (RHOC) Radiographers. The National Laboratories provide special technical support by providing technical support for training technical exercises, exercises, both in class and offsite locations.
Advanced

Nuclear Infrastructure Assessment and Disassembly (NID) Training
This training, conducted by DOD WMD through RHOC, provides the highest-fidelity overview of nuclear photography training for the Federal Radiological (RHOC) Radiographers. The National Laboratories provide special technical support by providing technical support for training technical exercises, exercises, both in class and offsite locations.
Advanced
<table>
<thead>
<tr>
<th>Course Name</th>
<th>Description</th>
<th>Level</th>
<th>Duration</th>
<th>Cost</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosive Breaching/Blast Effects</td>
<td>Instruction on explosive and mechanical breaching calculations, techniques and execution. Predicting explosive effects with software models.</td>
<td>Expert</td>
<td>4 hours</td>
<td>$3,000</td>
<td>In Person</td>
</tr>
<tr>
<td>Army 2A</td>
<td>Advanced Explosive Cybersecurity Awareness training.</td>
<td>Advanced</td>
<td>1 day</td>
<td></td>
<td>Web Based</td>
</tr>
<tr>
<td>Army 2B</td>
<td>Introduction to Metasys N2 controllers. Learn how the hardware interconnects, the protocol used for communication, and other relevant content that will be used to reinforce the selection and implementation of security controls relating specifically to ICS. The initial online version of this course will NOT include any lab exercises. The lab component of the course will be offered (in the future) as an optional purchase.</td>
<td>Fundamentals</td>
<td>28 hours</td>
<td>$2,250</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Industrial Cybersecurity Awareness for Executives and Managers</td>
<td>Raises awareness for your IT/OT specialists of current industrial cybersecurity trends and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.</td>
<td>Fundamentals</td>
<td>3 hours</td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>Industrial Cybersecurity Awareness Training for Executives and Managers</td>
<td>Helps executives and managers develop their awareness of current industrial cybersecurity issues and recent incidents, identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.</td>
<td>Fundamentals</td>
<td></td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>Advanced Industrial Cybersecurity Awareness Training for Executives and Managers</td>
<td>Helps your non-IT/OT specialists to increase their awareness of the current industrial cybersecurity issues by learning about ICS/OT differences and similarities, general cyber security basics and industrial cybersecurity specifics.</td>
<td>Novice</td>
<td></td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>Digital Forensics and Incident Response in ICS</td>
<td>Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments and to provide expert analysis and recommendations.</td>
<td>Intermediate</td>
<td>5 days</td>
<td></td>
<td>Web Based</td>
</tr>
<tr>
<td>Digital Forensics and Incident Response in ICS with in-depth practice</td>
<td>Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments and to provide expert analysis and recommendations.</td>
<td>Intermediate</td>
<td>10 days</td>
<td></td>
<td>Web Based</td>
</tr>
<tr>
<td>IoT Vulnerability Research and Exploitation</td>
<td>Raises awareness for your IT/OT specialists of current industrial cybersecurity trends and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.</td>
<td>Novice</td>
<td>3 days</td>
<td></td>
<td>Web Based</td>
</tr>
<tr>
<td>Industrial Cyber-Safety Games</td>
<td>On-site and online interactive training modules and cyber safety games conducted at all levels of technical expertise. These games are always modified for the appropriate levels of technical expertise ranging from executives and management to IT/OT personnel, to any employees who interact with industrial automation systems – production lines, in the control room or in the back office.</td>
<td>Intermediate</td>
<td>2 hours</td>
<td></td>
<td>Web Based</td>
</tr>
<tr>
<td>Understanding, Assessing and Securing Industrial Control Systems</td>
<td>Raises awareness for your IT/OT specialists of current industrial cybersecurity trends and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.</td>
<td>Novice</td>
<td>40 - 120 hours</td>
<td>$1,000</td>
<td>Online</td>
</tr>
<tr>
<td>Tempco DDC Fundamentals</td>
<td>This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical understanding of digital control systems.</td>
<td>Novice</td>
<td>36 hours</td>
<td>$750</td>
<td>Web Based</td>
</tr>
<tr>
<td>Metasys Extended Architecture for Building Operators</td>
<td>This three-day course teaches building personnel how to make the most effective and efficient use of the features of a Metasys® system extended architecture building management system. This course is for building personnel who have new installations of Metasys® system extended architecture using NAEs or NIEs or for those who have migrated from their existing Metasys® system.</td>
<td>Fundamentals</td>
<td>24 hours</td>
<td>$1,520</td>
<td>Web Based</td>
</tr>
<tr>
<td>Metasys Extended Architecture for Engineers</td>
<td>This three-day course teaches building personnel how to make the most effective and efficient use of the features of a Metasys® system extended architecture building management system. This course covers additional topics not covered in the Metasys® system extended architecture for Building Operators course.</td>
<td>Novice</td>
<td>28 hours</td>
<td>$2,250</td>
<td>Web Based</td>
</tr>
<tr>
<td>Introduction to Metasys® N2 Controllers</td>
<td>This course teaches building personnel how to make the most effective and efficient use of the features of a Metasys® system extended architecture building management system. This course covers additional topics not covered in the Metasys® system extended architecture for Building Operators course.</td>
<td>Novice</td>
<td>28 hours</td>
<td></td>
<td>Web Based</td>
</tr>
</tbody>
</table>

**CURRICULUM ANALYSIS THROUGH MACHINE LEARNING**

**41**
<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Duration</th>
<th>Cost</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metasys® FEC Operation/Troubleshooting</td>
<td>Designed as an overview course for people working with Field Equipment Controllers (FECs), this course shows students how to connect to FECs and how to download and test existing control programs. It also covers calibration of input sensors and setup and verification of inputs and outputs. This course is designed for building personnel who want to better understand field controller operation, commissioning and troubleshooting.</td>
<td>24 hours</td>
<td>$1,800</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Metasys System-Extended Architecture Hardware and Troubleshooting</td>
<td>This hands-on course provides experienced Metasys® users with valuable diagnostic and troubleshooting skills on system hardware. Discussions and exercises cover the full range of Metasys® network products, with an emphasis on communication solutions and other commonly experienced problems.</td>
<td>38 hours</td>
<td>$1,800</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Metasys® FEC Custom Programming</td>
<td>Students will learn how to create and test customized control strategies for FEC controllers in this three-day course. The course is designed for experienced building personnel who want to expand their knowledge of HVAC Control Systems and Johnson-Controls FEC devices. Although not a prerequisite, it is highly recommended that students are familiar with the topics found in course.</td>
<td>32 hours</td>
<td>$1,520</td>
<td>Advanced</td>
</tr>
<tr>
<td>Metasys® FEC Systems Engineering</td>
<td>In this advanced Field Equipment Controller (FEC) programming class, students will learn how to write and test programs for the FECs. They will use the software simulation tool to verify that the programs satisfy the sequence of operations. The course is designed for experienced personnel who want to become proficient in setting or running programs for Johnson Controls FEC devices.</td>
<td>24 hours</td>
<td>$1,520</td>
<td>Expert</td>
</tr>
<tr>
<td>Metasys System-Extended Architecture Engineering and Setup</td>
<td>Students will learn how to set up and manage the Network Automation Engine (NAE) database and to use the power of the System Configuration Tool to generate an NAE database from existing ASC controller programming.</td>
<td>38 hours</td>
<td>$2,250</td>
<td>Advanced</td>
</tr>
<tr>
<td>Metasys System-Extended Architecture Advanced Engineering</td>
<td>Experienced personnel will learn how to write advanced programs for facility-wide or specific mechanical control applications using the System Configuration Tool (SCT). Students will build, modify and troubleshoot routines they create.</td>
<td>24 hours</td>
<td>$1,800</td>
<td>Advanced</td>
</tr>
<tr>
<td>Graphics Generation Tool</td>
<td>This course teaches students how to create and modify the custom graphics used to both monitor and actively change building parameters and settings in a Metasys® automation system. It is a three-day online course which combines active instructor facilitation with student practice sessions with the facilitator available for questions. This course is for individuals interested in creating and editing Graphics Generation Tool (GGT) software.</td>
<td>24 hours</td>
<td>$1,200</td>
<td>Expert</td>
</tr>
<tr>
<td>TempleD DDC Fundamentals</td>
<td>This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.</td>
<td>36 hours</td>
<td>$1,250</td>
<td>Novice</td>
</tr>
<tr>
<td>FieldTech Basic</td>
<td>There are many different skill sets in the life of a field technician - engineering, IT infrastructure, technical support, and computer programming to name a few. Field Tech - Basic training will prepare field technicians to confidently install, commission, troubleshoot, and edit a WebCTRL system utilizing Eikon, SiteBuilder, ViewBuilder, and WebCTRL. Learners will become familiar with ISA submittal control drawings and the mechanical equipment these drawings represent. Hands-on tasks include hardware, networks, and software with an emphasis on real-life scenarios with the latest tools available.</td>
<td>36 hours</td>
<td>$1,000</td>
<td>Intermediate</td>
</tr>
<tr>
<td>WEBCTRL</td>
<td>This course is aimed at helping you leave the WebCTRL system or you've never attended a BASU course, this course is for you. From this course, you will be able to work with the WebCTRL user interface, create operators and privileges, develop schedules, troubleshoot with alarms and trends, and document with WebCTRL's report features. Higher end topics are also included.</td>
<td>24 hours</td>
<td>$1,500</td>
<td>Novice</td>
</tr>
<tr>
<td>EIKON</td>
<td>Learn the basics of EIKON programming. Learners who successfully complete this course will be able to identify the different types of microblocks, read a sequence of operations and translate to a program, simulate a program to find errors, and define microblock properties.</td>
<td>16 hours</td>
<td>$1,000</td>
<td>Novice</td>
</tr>
<tr>
<td>ViewBuilder - Basic</td>
<td>This course introduces Automated Logic-supplied area and equipment graphics. A complete ViewBuilder overview is covered, as well as its tools, controls, images, and available symbols. Custom topics include the use of conditional expressions and programming flowcharts. The learner will be able to successfully develop basic ViewBuilder graphics and provide common editing techniques to existing equipment and area graphics.</td>
<td>16 hours</td>
<td>$1,000</td>
<td>Novice</td>
</tr>
<tr>
<td>Networking - Basic</td>
<td>This course covers setup and troubleshooting techniques affiliated with basic Automated Logic networks. In addition, learners will build source trees, define and identify the fundamentals of IF, AND/ELSE, and NOT/IF networks, and how these concepts allow devices to communicate. Learners will also learn the basics of WintracK captures, clippings, and BACnet Discovery. Upon successful completion of this course, learners will be able to properly set up and troubleshoot basic Automated Logic networks, including the use of WintracK captures to capture IP traffic at the server, IF and AND/ELSE traffic at devices.</td>
<td>16 hours</td>
<td>$1,000</td>
<td>Novice</td>
</tr>
<tr>
<td>Commissioning - Intermediate</td>
<td>This course is designed to challenge the field technician with all aspects of a WebCTRL system. Upon completion of this course, the learner will be able to install and commission a WebCTRL system, provide functional testing of a control program, and apply the most advanced techniques of troubleshooting. The learner will also be responsible for turning in complete check out reports, installing add-ons, and correcting an entire system of common errors, including some obscure “gotchas,” using all of the skills the learner acquired in WebCTRL, Eikon, ViewBuilder, SiteBuilder, and EquipmentBuilder.</td>
<td>32 hours</td>
<td>$2,000</td>
<td>Intermediate</td>
</tr>
<tr>
<td>EIKON - Intermediate</td>
<td>Whether a Field Technician or Design Engineer, learners will expand on knowledge from the EIKON - Basic course to learn how to create complex control programs and logic symbols. The learners will be able to identify programming issues in a complex program. The learners will also be able to utilize naming standards to create a library for quickly placing previously developed logic into new systems, thus making programming more efficient. Building a detailed page, simulating a control program, major customization to equipment builder programs are among several other intermediate EIKON features offered in this course.</td>
<td>24 hours</td>
<td>$1,500</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Course</td>
<td>Description</td>
<td>Hours</td>
<td>Fee</td>
<td>Level</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>ViewBuilder - Intermediate</td>
<td>This course allows learners to create equipment graphics from a schematic drawing and technician pages. As an example, learners will be tasked to create one graphic for different types of similar equipment with the idea of creating a master graphic for all VAV's to shorten engineering time. In addition, learners will create a standard template for their company. Upon successful completion of this course, learners will be able to identify, define, and/or apply advanced conditional expressions, WebCTRL paths for system/equipment limiting, complete customization of equipment graphics including HTML links, external links, document links, internal links, and custom images and symbols for WebCTRL graphics.</td>
<td>24</td>
<td>$1,500</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Networking - Intermediate</td>
<td>As part of successful course completion, learners will set up complex AG networks, troubleshooting networks, and create a secure WebCTRL site. Learners will focus on troubleshooting WebCTRL system by reading a WebCTRL capture. This course is designed for individuals who need to design complex network systems as well as troubleshooting networks with Wireshark.</td>
<td>24</td>
<td>$1,500</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Third Party Integration BACon</td>
<td>BACon protocol has become the standard protocol within the Building Management Industry. Today, you will be hard-pressed to not find BACon in Building Automated Systems. In this course, a learner will not only learn how to seamlessly integrate third-party BACon controls into a WebCTRL system, but also understand the theory behind the BACon protocol. Learners will utilize ERIDON, Networking, and Viewbuilder skills to read and write BACon objects while following a sequence of operation to incorporate them into a WebCTRL system without stressing the network. A successful integration is never complete without commissioning the programming, graphic, and network. Automated Logic Technicians and Engineers will be equipped with tips and tricks to streamline integrating to multiple pieces of equipment and fine tune their BACon integration to achieve a healthy WebCTRL system, all with emphasis on efficiency.</td>
<td>24</td>
<td>$1,500</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Third Party Integration Modbus</td>
<td>Modbus protocol has been the protocol of industrial environment. Today, Modbus can be found in many industrial controls from energy metering to variable frequency drives. In this course, a learner will not only seamlessly integrate third-party Modbus controls into a WebCTRL system, but also understand the theory behind the Modbus protocol. Learners will utilize ERIDON, Networking, and Viewbuilder skills to read and write from/to Modbus registers while following a sequence of operation to incorporate them into a WebCTRL system without stressing the network. A successful integration is never complete without commissioning the programming, graphic, and network. Automated Logic Technicians and Engineers will be equipped with tips and tricks to streamline integrating to multiple pieces of equipment and fine tune their Modbus integration to achieve a healthy WebCTRL system, all with emphasis on efficiency.</td>
<td>24</td>
<td>$1,500</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Design Engineering - Basic</td>
<td>The foundation of every project starts here. This Design Engineering course will introduce the basic fundamentals of creating a complete WebCTRL system package to a field technician for installation. Learners will be challenged by completing a WebCTRL system throughout the entire project lifecycle. The project lifecycle will include the project scope, review of hardware, a control submittal developed with Engineering Design Suite, and creating a WebCTRL system database. This course strongly encourages the use of standards, the creation of libraries, and the optimal use of an engineer's time. With these skills the objective of the Design Engineer becomes clear: deliver on time, under budget, and mistake free. This course is for Automated Logic's branch and independent field office personnel only.</td>
<td>24</td>
<td>$1,500</td>
<td>Novice</td>
</tr>
<tr>
<td>Engineering Design Suite</td>
<td>The Advanced ViewBuilder's EDS add-on is a tool that allows you to streamline engineering tasks and the subsequent process to make drawings for installing and commissioning, create project reports, and control your revisions. The add-on includes built-in components with data sheets, engineering calculations and conversions, CO calculations for water and steam, a building floor manager, a schedule creator, and a searchable library in which you can add items. Data can be output to Microsoft Excel® in standalone spreadsheets or embedded in the Visio® EDS drawings. It provides automated creation of sequence of operation and your final drawing package.</td>
<td>16</td>
<td>$1,000</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Tempcon DDC Fundamentals</td>
<td>This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.</td>
<td>36</td>
<td>$550</td>
<td>Novice</td>
</tr>
<tr>
<td>Introduction to the Tracer SC System</td>
<td>This introduction course introduces you to the Tracer Synchrony interface and common tasks performed using it. This course provides a good introduction to many of the features of Tracer Ensemble as you walk through various real-life scenarios commonly encountered by a Tracer Ensemble building operator.</td>
<td>1.5</td>
<td>$0</td>
<td>Fundamentals</td>
</tr>
<tr>
<td>Tracer Ensemble for Operators</td>
<td>This course provides a good introduction to many of the features of Tracer Ensemble as you walk through various real-life scenarios commonly encountered by a Tracer Ensemble building operator.</td>
<td>1</td>
<td>$0</td>
<td>Fundamentals</td>
</tr>
<tr>
<td>Tracer ES Operations-Curriculum for Operators</td>
<td>This curriculum will walk the student through common tasks they would perform while using their Tracer ES building management system.</td>
<td>1.5</td>
<td>$0</td>
<td>Novice</td>
</tr>
<tr>
<td>Introduction to Computer Networking on Tracer Summit</td>
<td>This course provides the student the knowledge and skills needed to install a simple building automation system on a customer's existing network.</td>
<td>2</td>
<td>$0</td>
<td>Novice</td>
</tr>
<tr>
<td>Introduction to LonTalk</td>
<td>This course explains what LonTalk is, identifies the existing network management tools Trace and provides a basic understanding of technology and terminology. This course does not include use of third-party software to extract the ID of any other concepts not covered in the learning objectives.</td>
<td>2</td>
<td>$0</td>
<td>Novice</td>
</tr>
<tr>
<td>Tracer Ensemble Operation</td>
<td>Tracer Ensemble Operation is specifically designed for building operations and administrators to become more efficient with their Tracer Ensemble software which is a Web-enabled service and monitoring tool for multiple building facilities. Tracer Ensemble allows building operators and administrators access to Tracer Ensemble from the local network or the Internet to monitor and control their building system. Students will have the opportunity to work with the Tracer Ensemble software to become more familiar with common tools.</td>
<td>20</td>
<td>$1,120</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Tracer Synchrony Operation</td>
<td>In this Tracer Synchrony Operation course, students learn to operate and modify an installed Tracer SC system using the Synchrony interface. This highly interactive course includes presentations, demonstrations and hands-on workshops where students practice using the software applications integral to a Tracer SC's building management system.</td>
<td>20</td>
<td>$1,120</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Tracer Summit System Operation</td>
<td>In this course students will learn to perform common and advanced operations with their installed Tracer Summit building management system. This highly interactive basic course includes presentations and hands-on workshops where students practice using the common applications of a Tracer Summit building management system and learn how to monitor and control building mechanical systems.</td>
<td>20</td>
<td>$1,150</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Course Name</td>
<td>Description</td>
<td>Duration</td>
<td>Cost</td>
<td>Level</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>Tracer Summit Controls Service</td>
<td>The Tracer Synchrony Advanced Operation course builds on the knowledge and skills learned in the Tracer SC/Synchrony Operation course. This course will enable learners to expand their skills to complete a variety of advanced operations, control strategies and energy saving methods to get the most value out of their Tracer SC+ building control system.</td>
<td>36 hours</td>
<td>$1,980</td>
<td>Advanced</td>
</tr>
<tr>
<td>Tracer Synchrony Advanced Operation</td>
<td>This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.</td>
<td>24 hours</td>
<td>$1,120</td>
<td>Advanced</td>
</tr>
<tr>
<td>Advanced Tempcon DDC Fundamentals</td>
<td>This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.</td>
<td>24 hours</td>
<td>$1,950</td>
<td>Novice</td>
</tr>
<tr>
<td>Introduction to Desigo CC</td>
<td>This web-based training course provides an introduction to the Desigo CC Management Station.</td>
<td>0.5 hours</td>
<td>$0</td>
<td>Web-Based</td>
</tr>
<tr>
<td>Design CC Workstation I</td>
<td>Learn how to monitor and control your Design CC Management Station through hands-on guided exercises and discussions. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>24 hours</td>
<td>$1,950</td>
<td>Novice</td>
</tr>
<tr>
<td>Design CC Workstation II</td>
<td>The Design CC Workstation II course builds on the knowledge and skills learned in the Design CC Workstation I course. You will learn how to build and modify system objects. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>28 hours</td>
<td>$2,135</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Field Panel and FLN Operations</td>
<td>Learn to monitor, control and configure building automation systems locally from field panels and FLN devices using Datamate Advanced. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>28 hours</td>
<td>$1,816</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Field Panel and FLN Operations</td>
<td>Learn to monitor, control and configure building automation systems locally from field panels and FLN devices using Datamate Advanced. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>28 hours</td>
<td>$1,816</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Design CC Master Operator</td>
<td>Design CC Master Operator provides complex design and control programming scenarios for you to read, troubleshoot and correct. Upon successful completion of the training path, students will earn Master Programmer status.</td>
<td>24 hours</td>
<td>$1,950</td>
<td>Advanced</td>
</tr>
<tr>
<td>Introduction to Control Programming</td>
<td>This web-based training course covers the flow and functionality of creating building control programs.</td>
<td>0.5 hours</td>
<td>$0</td>
<td>Web-Based</td>
</tr>
<tr>
<td>PFC Programming I</td>
<td>Learn to develop and modify PFC programs. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>28 hours</td>
<td>$2,160</td>
<td>Intermediate</td>
</tr>
<tr>
<td>PFC Syntax Review</td>
<td>This web-based training course provides an introduction to the syntax and structure of PFC programs.</td>
<td>12 hours</td>
<td>$998</td>
<td>Novice</td>
</tr>
<tr>
<td>PFC Programming II</td>
<td>Learn to build and optimize PFC programs to improve building efficiency and incorporate staging and rotating of equipment. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.</td>
<td>28 hours</td>
<td>$2,135</td>
<td>Intermediate</td>
</tr>
<tr>
<td>PFC Master Programmer</td>
<td>This web-based training course provides an introduction to the syntax and structure of PFC programs.</td>
<td>24 hours</td>
<td>$1,950</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

CURRICULUM ANALYSIS THROUGH MACHINE LEARNING
Students will learn about the features of the Symphony/Infi90 Open control system and the Harmony Control Unit hardware components. Using a simple process control loop model as a base project, students will utilize Composer software tools to create a process control strategy. “Hands-on” exercises provide the opportunity for monitoring, tuning, and diagnostics of the Harmony Control Unit with Composer software.

40 hours $1,400 Intermediate

Harmony Configuration Strategies

This is an advanced course in which students will build upon their previous control system programming knowledge and implement control strategies to solve process control problems. Additionally, this course builds upon the knowledge acquired in M301, M311 or M321, and prepares the student for the Human System Interface course.

40 hours $1,500 Expert

SEL-351 RTAC

The APP 351 course is designed to be highly interactive and activity-based. During APP 351, in groups of two, you will configure a realistic communications scheme using the SEL-351 RTAC. Each section of this course will guide you, step-by-step, through configuring this communications scheme.

24 hours $1,425 Advanced

SEL-2032

Students will learn to use the SEL-2032 Communications Processor to design, create, and implement state-of-the-art subnet integration and automation system. Detailed hands-on exercises will show the ease with which you can apply the communications processor to both SEL relays and non-SEL IEDs. Students will explore use of the communications processor with DNP3 Level 2, Modbus, and the SEL-2701 Ethernet Processor. Multiplier applications of the communications processor are also addressed. Students (in groups of two) will gain hands-on experience in communicating, setting, and reporting functions directly with an SEL communications processor.

24 hours $1,425 Advanced

APP-351 or other relays

APP 351 provides comprehensive application training for the SEL-351 Protection System, an extremely flexible protective relay used by utilities worldwide, in multiple applications. Working in groups of two, students gain hands-on experience in communicating, setting, monitoring, retrieving event reports, and performing control functions by working directly with the SEL-351 Relay.

16 hours $950 Advanced

Power Meter Training Programs

The two day seminar offers practical training on how meters for customer, potential customers, and representatives. The training introduces you to the Nexus™ and Smart™ lines of power meters and monitors, with hands on setup and troubleshooting as an introduction to Communicator® advanced power monitoring and analysis software.

18 hours $900 Novice

Hardware Installation and Troubleshooting

PAC Operation Bundle

32 hours $1,134 Intermediate

PMU Admin and Maintenance

32 hours $1,576 Expert

GENESIS32 Standard or Basic

The GENESIS32 Standard course is a 5-day, hands-on, instructor-led class designed to provide you with the fundamentals of the GENESIS32 Automation Suite. You’ll become comfortable with OPC architecture and GENESIS32 modules including: Workbench32, Aliasing, Unified Data Manager, Security, creating Web-based applications, Enterprise Reporting, Charting and Analysis as well as the use of Multimedia Alarm notification, all in a secure GENESIS32 environment. The GENESIS32 platform is used to solve problems related to data acquisition and HMI (Human Machine Interface) aspects of the product. The course is designed to provide you with a good working knowledge of the GENESIS32 system.

40 hours $1,625 Intermediate

GENESIS44 + Dashboards

The GENESIS44 + Dashboards course is a 5-day, instructor-led class. The course is designed to provide students with a good working knowledge of the GENESIS32 Application Server and dashboards. All major features are covered from project configuration to data acquisition, visualization and deployment. Valuable hands-on lab exercises guide you through building and modifying the HMI/SCADA platform. This course also provides in-depth understanding of visualization for your facility data using dashboards, Workbench44 Advanced Features, Commanding and G2O SCADA mapping technology of EarthWorks. Specific ICONICS products used during this course include: GraphWorld44 for visualisation, AssetWork44, AssetWork44, TrendWorx44, ReportWork Express and PortalWorx.

40 hours $1,600 Intermediate

GENESIS44/Hyper Historian

The GENESIS44/Hyper Historian course is a 5-day, instructor-led class. This course is designed to provide students with a good working knowledge of the GENESIS44 Application Server and Hyper Historian. All major features are covered from project configuration to data acquisition, visualization and deployment. Valuable hands-on lab exercises guide you through building and modifying the HMI/SCADA platform. This course also provides fundamental design philosophy and concepts of Hyper Historian. The student will configure OPC, ODBC, database and other data points for collection, compression and storage. Learn how to utilize Hyper Historian performance calculations for custom data processing and how to visualize and report the results. Specific GENESIS44 products used during this course include: GraphWorld44, AssetWork44, AssetWork44, TrendWorx44, Hyper Historian and ReportWork Express.

40 hours $1,800 Intermediate

Building Basic Displays with PI Process Book

In this course, we will guide you on how to create a variety of PI Processbook displays, such as trends and graphs, to monitor your process. Additionally, this course leverages the power of the intuitive PI-AI avant architecture to enable you to display attributes of an asset, search in AI, and build element relative displays.

16 hours $159 Intermediate

Visualizing PI System Data with PI Vision

Learn how to build dynamic, graphical, interactive web-based dashboards with PI Vision. This well-paced online course is dedicated to a series of exercises where the student is challenged to solve real world problems using PI Vision.

24 hours $1,625 Intermediate
Enabling Condition Based Maintenance

The objectives of the course are to help your organization eliminate unnecessary maintenance, minimize unexpected failures, maximize use of resources, increase reliability and availability, and extend the lifetime of various assets using the OSIsoft PI System.

In this course, you will learn how to use AF templates, Event Frames and Asset Analytics to implement advanced logic to evaluate your equipment's health, as well as how to use notifications to receive automated alerts based on deviations in your process data. Additionally, you will learn how to use tools like PI Vision and PI DataLink to visualize important information about your equipment and make informed maintenance decisions.

Table 1: ‘Trainings’ spreadsheet in Randall Jung’s repository of cybersecurity courses.

<table>
<thead>
<tr>
<th>Training</th>
<th>Duration</th>
<th>Price</th>
<th>Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling Condition Based Maintenance</td>
<td>16 hours</td>
<td>$159</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Analyzing PI System Data</td>
<td>24 hours</td>
<td>$1,400</td>
<td>Advanced</td>
</tr>
</tbody>
</table>
Figure 1: Example of NICE Work-roles attributed to an input document (course description) with Cosine Similarity as percent match included.
Figure 2: Working example of model classification and output.
<table>
<thead>
<tr>
<th>KISA ID</th>
<th>Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0001</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>K0002</td>
<td>Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
</tr>
<tr>
<td>K0003</td>
<td>Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</td>
</tr>
<tr>
<td>K0004</td>
<td>Knowledge of cybersecurity and privacy principles.</td>
</tr>
<tr>
<td>K0005</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0006</td>
<td>Knowledge of specific operational impacts of cybersecurity lapses.</td>
</tr>
<tr>
<td>K0013</td>
<td>Knowledge of cyber defense and vulnerability assessment tools and their capabilities.</td>
</tr>
<tr>
<td>K0019</td>
<td>Knowledge of cryptography and cryptographic key management concepts.</td>
</tr>
<tr>
<td>K0027</td>
<td>Knowledge of organization's enterprise information security architecture.</td>
</tr>
<tr>
<td>K0028</td>
<td>Knowledge of organization's evaluation and validation requirements.</td>
</tr>
<tr>
<td>K0037</td>
<td>Knowledge of Security Assessment and Authorization process.</td>
</tr>
<tr>
<td>K0038</td>
<td>Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.</td>
</tr>
<tr>
<td>K0040</td>
<td>Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).</td>
</tr>
<tr>
<td>K0044</td>
<td>Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
<tr>
<td>K0048</td>
<td>Knowledge of Risk Management Framework (RMF) requirements.</td>
</tr>
<tr>
<td>K0049</td>
<td>Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).</td>
</tr>
<tr>
<td>K0054</td>
<td>Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.</td>
</tr>
<tr>
<td>K0059</td>
<td>Knowledge of new and emerging information technology (IT) and cybersecurity technologies.</td>
</tr>
<tr>
<td>K0070</td>
<td>Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflows, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, user-oriented attacks, malicious code).</td>
</tr>
<tr>
<td>K0284</td>
<td>Knowledge of structured analysis principles and methods.</td>
</tr>
<tr>
<td>K0389</td>
<td>Knowledge of systems diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>K0101</td>
<td>Knowledge of the organization’s enterprise information technology (IT) goals and objectives.</td>
</tr>
<tr>
<td>K0116</td>
<td>Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161).</td>
</tr>
<tr>
<td>K0146</td>
<td>Knowledge of the organization’s core business/mission processes.</td>
</tr>
</tbody>
</table>

Table 2: Reference spreadsheet from the Workforce Framework for cybersecurity.
Appendix D – External Programs

MIT-INL AI/ML 2021 Summer Symposium:

We enrolled in and attended INL and MIT’s collaborative Artificial Intelligence/Machine Learning 2021 Summer Symposium. Through the symposium lectures we were able to get a better grip on Python basics, latest Machine Learning libraries and packages, as well as an overall deeper understanding of AI/ML concepts and theories.

Intern Enrichment Series:

We took part in N&HS’ Intern Enrichment Series in which we were able to get better acquainted with INL and the many branches INL’s work touches by engaging with speakers who shared their unique experiences in their respective fields.

2021 Intern Poster Session:

We submitted a poster to INL’s Intern Poster Session in which our project is to be displayed at a high level for any interested party to observe.

ISCOP Briefings:

We had a chance to get feedback directly from industry professionals via biweekly ISCOP briefings. The comments we received were very insightful and helped us improve the way we communicate our project and problem statement.

CISA VLP Courses:

We were enrolled and completed the 100W, 210, 301V, and 401V training courses offered by CISA through the VLP. These courses introduced us to concepts within ICS cybersecurity, as well as the consequences and different relationships ICS has to IT and OT.