Registration form

SCADA 202 CEU Training Course $150.00
48 HOUR RUSH ORDER PROCESSING FEE ADDITIONAL $50.00

Start and Finish Dates: _____ *You will have 90 days from this date in order to complete this course*

List number of hours worked on assignment must match State Requirement. _____

Name_____Signature_____
I have read and understood the disclaimer notice on page 2. Digitally sign XXX

Address: _____

City_____State_____Zip_____

Email_____ Fax (_____) _____

Phone:
Home (_____) _____Work (_____) _____

Operator ID# _____Exp Date_____

Please circle/check which certification you are applying the course CEU's.
Water Treatment _____ Distribution _____ Collection _____

Wastewater Treatment_____ Other _____

Technical Learning College PO Box 3060, Chino Valley, AZ 86323
Primary Fax (928) 272-0747 info@tlch2o.com
Telephone (928) 468-0665 Toll Free (866) 557-1746

If you've paid on the Internet, please write your Customer#_____

Please invoice me, my PO#_____

Please pay with your credit card on our website under Bookstore or Buy Now. Or call us and provide your credit card information.

DISCLAIMER NOTICE
I understand that it is my responsibility to ensure that this CEU course is either approved or accepted in my State for CEU credit. I understand State laws and rules change on a frequent basis and I believe this course is currently accepted in my State for CEU or contact hour credit, if it is not, I will not hold Technical Learning College responsible. I also understand that this type of study program deals with dangerous conditions and that I will not hold Technical Learning College, Technical Learning Consultants, Inc. (TLC) liable for any errors or omissions or advice contained in this CEU education training course or for any violation or injury caused by this CEU education training course material. I will call or contact TLC if I need help or assistance and double-check to ensure my registration page and assignment has been received and graded.

Professional Engineers; Most states will accept our courses for credit but we do not officially list the States or Agencies. Please check your State for approval.

You can obtain a printed version of the course from TLC for an additional $59.95 plus shipping charges.

AFFIDAVIT OF EXAM COMPLETION
I affirm that I personally completed the entire text of the course. I also affirm that I completed the exam without assistance from any outside source. I understand that it is my responsibility to file or maintain my certificate of completion as required by the state or by the designation organization.

Grading Information
In order to maintain the integrity of our courses we do not distribute test scores, percentages or questions missed. Our exams are based upon pass/fail criteria with the benchmark for successful completion set at 70%. Once you pass the exam, your record will reflect a successful completion and a certificate will be issued to you.

Do not solely depend on TLC's Approval list for it may be outdated.

All downloads are electronically tracked and monitored for security purposes.

Some States and many employers require the final exam to be proctored.
http://www.abctlc.com/downloads/PDF/PROCTORFORM.pdf

No refunds.

We will stop mailing the certificate of completion we need your e-mail address. We will e-mail the certificate to you, if no e-mail address; we will mail it to you.

SCADA 202 CEU Course Answer Key

Name _____

Telephone # _____

You are solely responsible in ensuring that this course is accepted for credit by your State. <u>No refunds.</u> Did you check with your State agency to ensure this course is accepted for credit?

Method of Course acceptance confirmation. Please fill this section

Website __ Telephone Call___ Email____ Spoke to_____

Do not solely depend on TLC's Approval list for it may be outdated.

What is the approval number if Applicable? _____

Please circle, underline, bold or X only one correct answer

1. A B
2. A B
3. A B
4. A B
5. A B
6. A B
7. A B
8. A B
9. A B
10. A B
11. A B C D
12. A B C D
13. A B C D
14. A B C D
15. A B C D
16. A B C D
17. A B C D
18. A B C D
19. A B C D
20. A B C D
21. A B C D
22. A B C D
23. A B C D
24. A B C D
25. A B C D
26. A B C D
27. A B C D
28. A B C D
29. A B C D
30. A B C D
31. A B C D
32. A B C D
33. A B C D
34. A B C D
35. A B
36. A B
37. A B
38. A B
39. A B
40. A B
41. A B
42. A B
43. A B
44. A B
45. A B
46. A B C D E F
47. A B C D E F
48. A B C D E F
49. A B C D E F
50. A B C D E F
51. A B C D E F
52. A B C D E F
53. A B C D E F
54. A B C D E F

55. A B C D E F
56. A B C D E F
57. A B C D E F
58. A B C D E F
59. A B C D E F
60. A B C D E F
61. A B C D E F
62. A B C D E F
63. A B C D E F
64. A B C D E F
65. A B C D E F
66. A B C D E F
67. A B C D E F
68. A B C D E F
69. A B C D E F
70. A B C D E F
71. A B C D E F
72. A B C D E F
73. A B C D E F
74. A B C D E F
75. A B C D E F
76. A B C D E F
77. A B C D E F
78. A B C D E F
79. A B C D E F
80. A B C D E F
81. A B C D E F
82. A B C D E F
83. A B C D E F
84. A B C D E F
85. A B C D E F
86. A B C D E F
87. A B C D E F
88. A B C D E F
89. A B C D E F
90. A B C D E F
91. A B C D E F
92. A B C D E F
93. A B C D E F
94. A B C D E F
95. A B C D E F
96. A B C D E F
97. A B C D E F
98. A B C D E F
99. A B C D E F
100. A B C D E F
101. A B C D E F
102. A B C D E F
103. A B C D E F
104. A B C D E F
105. A B C D E F
106. A B C D E F
107. A B C D E F
108. A B C D E F
109. A B C D E F
110. A B C D E F
111. A B C D E F
112. A B C D E F
113. A B C D E F
114. A B C D E F
115. A B C D E F
116. A B C D E F
117. A B C D E F
118. A B C D E F
119. A B C D E F
120. A B C D E F
121. A B C D E F
122. A B C D E F
123. A B C D E F
124. A B C D E F
125. A B C D E F
126. A B C D E F
127. A B C D E F
128. A B C D E F
129. A B C D E F
130. A B C D E F
131. A B C D E F
132. A B C D E F
133. A B C D E F
134. A B C D E F
135. A B C D E F
136. A B C D E F
137. A B C D E F
138. A B C D E F
139. A B C D E F
140. A B C D E F
141. A B C D E F
142. A B C D E F
143. A B C D E F
144. A B C D E F
145. A B C D E F
146. A B C D E F
147. A B C D E F
148. A B C D E F
149. A B C D E F
150. A B C D E F

151. A B C D E F
152. A B C D E F
153. A B C D E F
154. A B C D E F
155. A B C D E F
156. A B C D E F
157. A B C D E F
158. A B C D E F
159. A B C D E F
160. A B C D E F
161. A B C D E F
162. A B C D E F
163. A B C D E F
164. A B C D E F
165. A B C D E F
166. A B C D E F
167. A B C D E F
168. A B C D E F
169. A B C D E F
170. A B C D E F
171. A B C D E F
172. A B C D E F
173. A B C D E F
174. A B C D E F
175. A B C D E F
176. A B C D E F
177. A B C D E F
178. A B C D E F
179. A B C D E F
180. A B C D E F
181. A B C D E F
182. A B C D E F
183. A B C D E F
184. A B C D E F
185. A B C D E F
186. A B C D E F
187. A B C D E F
188. A B C D E F
189. A B C D E F
190. A B C D E F
191. A B C D E F
192. A B C D E F
193. A B C D E F
194. A B C D E F
195. A B C D E F
196. A B C D E F
197. A B C D E F
198. A B C D E F
199. A B C D E F
200. A B C D E F
201. A B C D E F
202. A B C D E F
203. A B C D E F
204. A B C D E F
205. A B C D E F
206. A B C D E F
207. A B C D E F
208. A B C D E F
209. A B C D E F
210. A B C D E F
211. A B C D E F
212. A B C D E F
213. A B C D E F
214. A B C D E F
215. A B C D E F
216. A B C D E F
217. A B C D E F
218. A B C D E F
219. A B C D E F
220. A B C D E F
221. A B C D E F
222. A B C D E F
223. A B C D E F
224. A B C D E F
225. A B C D E F
226. A B C D E F
227. A B C D E F
228. A B C D E F
229. A B C D E F
230. A B C D E F
231. A B C D E F
232. A B C D E F
233. A B C D E F
234. A B C D E F
235. A B C D E F
236. A B C D E F
237. A B C D E F
238. A B C D E F
239. A B C D E F
240. A B C D E F
241. A B C D E F
242. A B C D E F
243. A B C D E F
244. A B C D E F
245. A B C D E F
246. A B C D E F

247. A B C D E F
248. A B C D E F
249. A B C D E F
250. A B C D E F
251. A B C D E F
252. A B C D E F
253. A B C D E F
254. A B C D E F
255. A B C D E F
256. A B C D E F
257. A B C D E F
258. A B C D E F
259. A B C D E F
260. A B C D E F
261. A B C D E F
262. A B C D E F
263. A B C D E F
264. A B C D E F
265. A B C D E F
266. A B C D E F
267. A B C D E F
268. A B C D E F
269. A B C D E F
270. A B C D E F
271. A B C D E F
272. A B C D E F
273. A B C D E F
274. A B C D E F
275. A B C D E F
276. A B C D E F
277. A B C D E F
278. A B C D E F
279. A B C D E F
280. A B C D E F
281. A B C D E F
282. A B C D E F
283. A B C D E F
284. A B C D E F
285. A B C D E F
286. A B C D E F
287. A B C D E F
288. A B C D E F
289. A B C D E F
290. A B C D E F
291. A B C D E F
292. A B C D E F
293. A B C D E F
294. A B C D E F
295. A B C D E F
296. A B C D E F
297. A B C D E F
298. A B C D E F
299. A B C D E F
300. A B C D E F

Disclaimer

I understand that this course will cover general laws, regulations, required procedures and work rules relating to SCADA and electrical principles. It should be noted, however, that the federal and state regulations are an ongoing process and subject to change over time. This course is a continuing education course for employees who are learning general electrical principles but are not allowed to work on electrical projects unless qualified or licensed. It is not designed to meet the full requirements of the Department of Labor-Occupational Safety and Health Administration (OSHA) rules and regulations. Only qualified licensed electricians should be allowed to work on any or all electrical installations or components. This course will not qualify you to work on any type of electrical system or component.

Signature _____

Additional certificate for another Agency – additional fee $50

Please e-mail or fax this survey along with your final exam

SCADA 202 CEU TRAINING COURSE
CUSTOMER SERVICE RESPONSE CARD

NAME: _____

E-MAIL_____PHONE_____

PLEASE COMPLETE THIS FORM BY CIRCLING THE NUMBER OF THE APPROPRIATE ANSWER IN THE AREA BELOW.

Please rate the difficulty of your course.
Very Easy 0 1 2 3 4 5 Very Difficult

Please rate the difficulty of the testing process.
Very Easy 0 1 2 3 4 5 Very Difficult

Please rate the subject matter on the exam to your actual field or work.
Very Similar 0 1 2 3 4 5 Very Different

How did you hear about this Course? _____

What would you do to improve the Course?

_____

_____

How about the price of the course? Poor __ Fair__ Average__ Good __ Great __

How was your customer service? Poor __ Fair__ Average__ Good __ Great __

Any other concerns or comments.

_____

_____

_____

Please fax the answer key to TLC
(928) 272-0747

Rush Grading Service
If you need this assignment graded and the results mailed to you within a 48-hour period, prepare to pay an additional rush service handling fee of $50.00. This fee may not cover postage costs. If you need this service, simply write RUSH on the top of your Registration Form. We will place you in the front of the grading and processing line. Thank you…

SCADA 202 CEU Course Assignment

The Assignment (Exam) is also available in Word on the Internet for your Convenience, please visit www.ABCTLC.com and download the assignment and e- mail it back to TLC.

You will have 90 days from the start of this course to complete in order to receive your Professional Development Hours (**PDHs**) or Continuing Education Unit (**CEU**). A score of 70 % is necessary to pass this course. We prefer if this exam is proctored. No intentional trick questions. If you should need any assistance, please email all concerns and the completed manual to info@tlch2o.com.

We would prefer that you utilize the enclosed answer sheet in the front, but if you are unable to do so, type out your own answer key. Please include your name and address on your Answer Key and make copy for yourself. You can e-mail or fax your Answer Key along with the Registration Form to TLC. **(S) Means answer may be plural or singular**. **Multiple Choice Section, One answer per question and please use the answer key.**

Topic 1 – SCADA Introduction

1. Industrial organizations and companies in the public and private sectors to maintain and control efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime utilize SCADA systems.
A. True B. False

2. SCADA systems are critical for industrial organizations (like water and wastewater facilities) since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.
A. True B. False

3. The SCADA software will process, distribute, and display important data, helping operators and other employees understand the data and make important decisions.
A. True B. False

4. The acronym SCADA refers to the centralized computer systems that control and monitor the entire sites, or they are the complex systems spread out over large areas. Nearly all the control actions are automatically performed by the remote terminal units (RTUs) or by the programmable logic controllers (PLCs).
A. True B. False

5. Data acquisition starts at the HMI level, which includes the equipment status reports, and meter readings. Data is then formatted in such way that the operator of the control room can make the supervisory decisions to override or adjust normal HMI controls, by using the PLC.
A. True B. False

6. SCADA systems implement the distributed databases known as Excel databases, containing data elements called rows or columns.
A. True B. False

7. The key attribute of a SCADA system is its capability to perform a supervisory operation over a variety of other proprietary devices.
A. True B. False

8. The internet is linked to the SCADA system's databases, to provide the diagnostic data, management information and trending information such as logistic information, detailed schematics for a certain machine or sensor, maintenance procedures and troubleshooting guides.
A. True B. False

9. The HMI, or Human Machine Interface, is a device apparatus that gives the processed data to the human operator. A human operator uses HMI to control processes.
A. True B. False

10. The information provided by the HMI to the operating personnel is graphical, in the form of mimic diagrams. This means the schematic representation of the plant that is being controlled is obtainable to the operator.
A. True B. False

11. Which of the following terms can convert electrical signals coming from the equipment into digital values like the status- open/closed – from a valve or switch, or the measurements like flow, pressure, current or voltage?
A. RTU C. PLC
B. HMI D. None of the Above

12. By converting and sending the electrical signals to the equipment, _____ may control the equipment, like closing or opening a valve or a switch, or setting the speed of the pump.
A. RTU C. SCADA system
B. HMI D. None of the Above

13. A 'supervisory Station' refers to the software and servers responsible for communication with the field equipment (PLCs, RTUs etc.), and after that, to _____ software running on the workstations in the control room, or somewhere else.
A. RTU C. SCADA system
B. HMI D. None of the Above

14. Which of the following terms can have multiple servers, disaster recovery sites and distributed software applications in larger SCADA systems?
A. Master station C. SCADA system(s)
B. SCADA implementation(s) D. None of the Above

15. For increasing the system integrity, _____are occasionally configured in hot standby or dual-redundant formation, providing monitoring and continuous control during server failures.
A. Multiple servers C. Multiple stations
B. Independent systems D. None of the Above

16. Which of the following terms originally used modem connections or combinations of direct and radio serial to meet communication requirements, even though IP and Ethernet over SONET/SDH can also be used at larger sites like power stations and railways?
A. SCADA systems C. SCADA
B. SCADA implementation(s) D. None of the Above

17. The monitoring function or remote management of the _____ is referred to as telemetry.
A. SCADA operator C. SCADA system(s)
B. SCADA implementation(s) D. None of the Above

18. An important part of most SCADA implementations is _____. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred.
A. Policies and procedures C. Alarm handling
B. The cyber security team D. None of the Above

19. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or _____are informed).
A. SCADA operator C. Remote SCADA operators
B. SCADA implementation(s) D. None of the Above

20. In many cases, a _____ may have to recognize the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared.
A. SCADA operator C. SCADA
B. SCADA implementation(s) D. None of the Above

21. Which of the following terms might automatically monitor whether the value in an analogue point lies outside high and low- limit values associated with that point?
A. SCADA operator C. SCADA system(s)
B. SCADA implementation(s) D. None of the Above

22. Which of the following terms translates the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current? By translating and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.
A. RTU C. PLCs
B. HMI D. None of the Above

23. In the first production, mainframe systems were used for computing. At the time SCADA was established, networks did not exist. Therefore, the _____ did not have any connectivity to other systems, meaning they were independent systems.
A. SCADA systems C. Multiple stations
B. Independent systems D. None of the Above

24. The information between multiple stations was shared in real time through _____ and the processing was distributed between various multiple stations. The cost and size of the stations were reduced in comparison to the ones used in the first generation.
A. RTU C. LAN
B. HMI D. None of the Above

25. The interaction between the system and the master station is done through the WAN protocols like the_____.
A. Internet Protocols (IP) C. Remote or distant operation
B. Common IT practices D. None of the Above

26. Since the standard protocols used and the _____ can be accessed through the internet, the vulnerability of the system is enlarged.
A. Networked SCADA systems C. SCADA system(s)
B. SCADA implementation(s) D. None of the Above

27. SCADA systems are now in line with the standard networking technologies. The old proprietary standards are being replaced by the_____. However, due to certain characteristics of frame-based network communication technology, Ethernet networks have been recognized by the majority of markets for HMI SCADA.
A. ICS network C. TCP/IP and Ethernet protocols
B. LAN to a WAN D. None of the Above

28. There are many threat vectors to a modern SCADA system. One is the threat of unauthorized access to the control software, whether it is human access or changes induced intentionally or accidentally by _____residing on the control host machine.
A. Policies and procedures C. Virus infections and other software threats
B. DoS attacks and malware D. None of the Above

29. In many cases, SCADA users have assumed that having a VPN offered sufficient protection, unaware that security can be _____to SCADA-associated network jacks and switches.
A. Different risks and priorities C. Trivially bypassed with physical access
B. Significantly less isolation D. None of the Above

30. Industrial control vendors propose approaching SCADA security like _____ with a defense in depth strategy that leverages common IT practices.
A. Remote control tasks C. Remote or distant operation
B. Information Security D. None of the Above

31. A SCADA (or supervisory control and data acquisition) system means a system consisting of a number of remote terminal units (or RTUs) collecting field data connected back to a master station via a_____.
A. Communications system C. PLCs, RTUs etc.
B. HMI D. None of the Above

32. The master station displays the _____and also allows the operator to implement remote control tasks.
A. Acquired data C. Remote or distant operation
B. Common IT practices D. None of the Above

33. The accurate and timely data (normally real-time) allows for optimization of the operation of the plant and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier _____.

A. Remote control tasks C. Remote or distant operation
B. Non-automated systems D. None of the Above

34. There is a fair degree of misunderstanding between the definition of SCADA systems and process control system. SCADA has the_____.

A. Remote control tasks C. Connotation of remote or distant operation
B. Non-automated systems D. None of the Above

Topic 2 - SCADA, HMI, DCS, and PLCs Section

35. Field devices regulate local processes such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

A. True B. False

36. PLCs are incorporated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of a localized process.

A. True B. False

37. Product and process control are typically achieved by deploying feed back or feed forward control loops whereby key product and/or process conditions are automatically maintained around a desired set point.

A. True B. False

38. To accomplish the chosen product and/or process tolerance around a specified set point, specific programmable controllers (PLC) are employed in the field and proportional, integral, and/or differential settings on the PLC are tuned to provide the desired tolerance as well as the rate of self-correction during process upsets.

A. True B. False

39. PLCs are mechanical-based analog devices that control industrial equipment and processes.

A. True B. False

40. While PLCs are control system components used all over SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide regulatory control of discrete processes such as automobile assembly lines and power plant soot blower controls. PLCs are used extensively in almost all industrial and water treatment processes.

A. True B. False

41. PLC processes have distinct processing steps, conducted on a quantity of material. There is no distinct start and end step to a batch process.

A. True B. False

42. The discrete-based manufacturing industries typically conduct a series of steps on a single device to create the end-product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry.
A. True B. False

43. DCS and PLC communications are typically carried out using Wi-Fi technologies that are typically more reliable and high speed compared to the short-distance communication systems used by SCADA systems.
A. True B. False

44. A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables.
A. True B. False

45. Uncontrolled variables are transmitted to the controller from the sensors.
A. True B. False

46. Which of the following missing terms understands the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators?
A. Policies and procedures D. Cyber security programs
B. The cyber security team E. The controller
C. Physical impacts F. None of the Above

47. Process changes from disturbances result in new sensor signals, recognizing the state of the process, to again be transmitted to _____.
A. The controller D. PLC(s)
B. HMI E. Remote Terminal Unit or (RTU)
C. An IED F. None of the Above

48. Operators and engineers use _____ to construct set points, control algorithms, and adjust and establish parameters in the controller.
A. Controller D. Remote Terminal Unit or (RTU)
B. HMI(s) E. PLC(s)
C. SCADA Server F. None of the Above

49. Which of the following missing terms also displays process status information and historical information?
A. Controller D. Remote Terminal Unit or (RTU)
B. HMI(s) E. PLC(s)
C. SCADA Server F. None of the Above

50. Which of the following missing terms contains a proliferation of control loops, HMIs, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures.
A. Data historian D. PLC(s)
B. HMI E. ICS
C. An IED F. None of the Above

51. Which of the following missing terms is the device that preforms as the master in a SCADA system? Remote terminal units and PLC devices located at remote field sites typically act as slaves.

A. Controller
B. HMI(s)
C. SCADA Server
D. Remote Terminal Unit or (RTU)
E. PLC(s)
F. None of the Above

52. Which of the following missing terms also called a remote telemetry unit, is special purpose data acquisition and control unit designed to support SCADA remote stations?

A. Data historian
B. HMI
C. An IED
D. PLC(s)
E. Remote Terminal Unit or (RTU)
F. None of the Above

53. Which of the following missing terms are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unobtainable?

A. Controller
B. HMI(s)
C. SCADA Server
D. RTU
E. PLC(s)
F. None of the Above

54. Which of the following missing terms is a small industrial computer originally designed to implement the logic functions executed by electrical hardware (relays, drum switches, and mechanical timer/counters)?

A. Data historian
B. HMI
C. An IED
D. PLC
E. Remote Terminal Unit or (RTU)
F. None of the Above

55. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than _____.

A. Controller
B. HMI(s)
C. SCADA Server
D. Special-purpose RTUs
E. PLC(s)
F. None of the Above

56. Which of the following missing terms is a “smart” sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and implement local processing and control?

A. Data historian
B. HMI
C. An IED
D. PLC(s)
E. Remote Terminal Unit or (RTU)
F. None of the Above

57. Which of the following missing terms in SCADA and DCS systems allows for automatic control at the local level?

A. Controller
B. HMI(s)
C. SCADA Server
D. Remote Terminal Unit or (RTU)
E. An IED
F. None of the Above

58. Which of the following missing terms is software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations?

A. Data historian
B. HMI
C. An IED
D. PLC(s)
E. Remote Terminal Unit or (RTU)
F. None of the Above

59. The HMI also displays_____, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Process status information
E. Centralized monitoring
F. None of the Above

60. The data historian is a centralized database for logging all process information within an ICS. Information stored in this database can be accessed to support various analyses, from statistical process control to_____.

A. Policies and procedures
B. Enterprise level planning
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

61. The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as _____.

A. ICS network
B. LAN to a WAN
C. Between two networks
D. Router
E. PLCs, RTUs and IEDs
F. None of the Above

62. Which of the following missing terms can reside on the control server or on a separate computer platform?

A. An IO server
B. Network
C. Data historian
D. Fieldbus technologies
E. Supervisory control level
F. None of the Above

63. The fieldbus network links sensors and other devices to a _____ or other controller.

A. ICS network
B. LAN to a WAN
C. Between two networks
D. Router
E. PLC
F. None of the Above

64. Which of the following missing terms eliminates the need for point-to-point wiring between the controller and each device?

A. An IO server
B. Network
C. Data historian
D. Fieldbus technologies
E. Supervisory control level
F. None of the Above

65. The sensors communicate with the fieldbus controller using a_____. The messages sent between the sensors and the controller uniquely identify each of the sensors.

A. ICS network
B. LAN to a WAN
C. Specific protocol
D. Router
E. PLCs, RTUs and IEDs
F. None of the Above

66. Which of the following missing terms connects the supervisory control level to lower-level control modules?

A. The control network
B. Network
C. Data historian
D. Fieldbus technologies
E. Supervisory control level
F. None of the Above

67. Which of the following missing terms is a communications device that transfers messages between two networks?

A. ICS network
B. LAN to a WAN
C. Between two networks
D. Router
E. PLCs, RTUs and IEDs
F. None of the Above

68. Common uses for routers include connecting a _____, and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.

A. ICS network
B. LAN to a WAN
C. Between two networks
D. Router
E. PLCs, RTUs and IEDs
F. None of the Above

69. Which of the following missing terms protects devices on a network by monitoring and controlling communication packets using predefined filtering policies?

A. An IO server
B. A firewall
C. Data historian
D. Fieldbus technologies
E. Supervisory control level
F. None of the Above

70. Firewalls are also useful in managing_____.

A. ICS network
B. LAN to a WAN
C. Between two networks
D. Router
E. ICS network segregation strategies
F. None of the Above

71. Which of the following missing terms are distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data?

A. Remote access points
B. Network
C. Data historian
D. Fieldbus technologies
E. Supervisory control level
F. None of the Above

72. SCADA systems are used to control _____where centralized data acquisition is as important as control.

A. Dispersed assets
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

73. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a _____for numerous process inputs and outputs.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Centralized monitoring and control system
E. Centralized monitoring
F. None of the Above

74. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to _____an entire system from a central location in real time.

A. Send new set points
B. Radio telemetry
C. Channel sharing
D. Monitor or control
E. Communicate directly
F. None of the Above

75. The MTU stores and processes the information from RTU inputs and outputs, while the RTU or PLC_____.

A. Controls the local process
B. Direct instructions
C. Control dispersed assets
D. Processes the information
E. Centralizes monitoring
F. None of the Above

76. An IED, such as a protective relay, may communicate directly to the SCADA master station, or a local RTU may poll the IEDs to collect the data and_____.

A. Send new set points
B. Radio telemetry
C. Channel sharing
D. Pass it to the SCADA master station
E. Communicate directly
F. None of the Above

77. IEDs provide a _____to control and monitor equipment and sensors. IEDs may be directly polled and controlled by the SCADA master station and in most cases have local programming that allows for the IED to act without direct instructions from the SCADA control center.

A. Direct interface
B. Direct instructions
C. Control disperse interface
D. Processes the information
E. Centralized monitoring
F. None of the Above

78. SCADA systems are typically designed to be fault-tolerant systems with _____into the system architecture.

A. Sending new set points
B. Radio telemetry
C. Channel sharing
D. Significant redundancy built
E. Communicate directly
F. None of the Above

79. Field sites are often equipped with a _____to allow field operators to implement remote diagnostics and repairs typically over a separate dial up or WAN connection.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Remote access capability
E. Centralized monitoring
F. None of the Above

80. _____the simplest type; however, it is expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of SCADA operations.

A. Point-to-point is functionally
B. Radio telemetry
C. Channel sharing
D. Redundancy
E. Communicate directly
F. None of the Above

81. The series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and_____.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Increased system complexity
E. Centralized monitoring
F. None of the Above

82. Point-to-point connections are used for all control center to field site communications, with _____.

A. Send new set points
B. Radio telemetry
C. Channel sharing
D. Redundancy
E. Two connections using radio telemetry
F. None of the Above

83. A regional control center sits above the primary control center for a higher level of supervisory control. The corporate network has access to all control centers through the WAN, and field sites can be accessed remotely for_____.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Processing the information
E. Troubleshooting and maintenance operations
F. None of the Above

84. The primary control center polls field devices for data at defined intervals (e.g., 5 seconds, 60 seconds, etc.) and can send _____ to a field device as required.

A. New set points
B. Radio telemetry
C. Channel sharing
D. Redundancy
E. Communicate directly
F. None of the Above

85. In addition to polling and issuing high-level commands, the SCADA server also watches for _____ coming from field site alarm systems.

A. Remote diagnostics
B. Direct instructions
C. Control dispersed assets
D. Priority interrupts
E. Centralized monitoring
F. None of the Above

86. In the case of SCADA systems, they provide the same functionality of RTUs. When used in DCSs, PLCs are implemented as local controllers within a_____.

A. Supervisory control scheme
B. Cyber security team
C. Physical impacts
D. Cyber security program
E. DoS attack
F. None of the Above

87. Which of the following missing terms are also implemented as the primary components in smaller control system configurations?

A. DCSs
B. SCADA control technology
C. RTUs
D. Geographically remote field control stations
E. PLCs
F. None of the Above

88. Both the electrical power transmission and distribution grid industries use _____technology to operate highly interconnected and dynamic systems consisting of thousands of public and private utilities and rural cooperatives for supplying electricity to end users.

A. DCSs
B. SCADA control technology
C. RTUs
D. Geographically remote field control stations
E. Geographically distributed SCADA control
F. None of the Above

89. SCADA systems monitor and control electricity distribution by collecting data from and issuing commands to _____ from a centralized location.

A. DCSs
B. SCADA control technology
C. RTUs
D. Geographically remote field control stations
E. Geographically distributed SCADA control
F. None of the Above

90. Which of the following missing terms are often tied together? This is the case for electric power control centers and electric power generation facilities. Although the electric power generation facility operation is controlled by a DCS, the DCS must communicate with the SCADA system to coordinate production output with transmission and distribution demands.

A. DCSs
B. SCADA control technology
C. RTUs
D. SCADA systems and DCSs
E. PLCs
F. None of the Above

Topic 3 - ICS Characteristics, Threats and Vulnerabilities

91. Most Industrial Control Systems (ICSs) in use today were established years ago, long before public and private networks, desktop computing, or the Internet were a common part of_____ .

A. Different risks and priorities
B. Business operations
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Unexpected outages of systems
F. None of the Above

92. Initially, ICSs had little resemblance to IT systems in that ICSs were isolated systems running proprietary control protocols using_____.

A. Outages
B. Deterministic responses
C. New security solutions
D. Adopting IT solutions
E. Specialized hardware and software
F. None of the Above

93. Widely obtainable, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of _____.

A. Different risks and priorities
B. Significantly less isolation
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Unexpected outages of systems
F. None of the Above

94. As ICSs are adopting IT solutions to promote corporate connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble_____.

A. IT systems
B. Deterministic responses
C. New security solutions
D. IT solutions
E. Specialized hardware and software
F. None of the Above

95. This integration supports_____, but it provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these systems.

A. Policies and procedures
B. New IT capabilities
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

96. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, _____ are needed that are tailored to the ICS environment.

A. Outages
B. Deterministic responses
C. New security solutions
D. Adopting IT solutions
E. Specialized hardware and software
F. None of the Above

97. ICSs have many characteristics that differ from traditional Internet-based information processing systems, including _____.

A. Different risks and priorities
B. Significantly less isolation
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Unexpected outages of systems
F. None of the Above

98. ICSs are generally time-critical; delay is not acceptable for the delivery of information, and high throughput is typically not essential. In contrast, IT systems typically require high throughput, but they can typically withstand_____.

A. Outages
B. Deterministic responses
C. New security solutions
D. Substantial levels of delay and jitter
E. Specialized hardware and software
F. None of the Above

99. ICSs must display _____.

A. Outages
B. Deterministic responses
C. New security solutions
D. IT solutions
E. Specialized hardware and software
F. None of the Above

100. Many ICS processes are continuous in nature. _____that control industrial processes are not acceptable.

A. Different risks and priorities
B. Significantly less isolation
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Unexpected outages of systems
F. None of the Above

101. Which of the following terms often must be planned and scheduled days/weeks in advance?

A. Outages
B. Deterministic responses
C. New security solutions
D. Adopting IT solutions
E. Specialized hardware and software
F. None of the Above

102. In a typical IT system, data confidentiality and integrity are typically the primary concerns. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or _____are the primary concerns.

A. Different risks and priorities
B. Lost or damaged products
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Safety and security
F. None of the Above

103. The personnel responsible for operating, securing, and maintaining ICSs must understand the link between_____.

A. Different risks and priorities
B. Lost or damaged products
C. Safety and security
D. Cyber security vulnerabilities and incidents
E. Safety and security
F. None of the Above

104. In a typical IT system, the primary focus of security is protecting the operation of IT assets, whether_____, and the information stored on or transmitted among these assets.

A. Current security capabilities
B. Centralized or distributed
C. More difficult to upgrade
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

105. In some architectures,_____ and processed centrally is more critical and is afforded more protection.

A. Current security capabilities
B. Information stored
C. More difficult to upgrade
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

106. For ICSs, _____(e.g., PLC, operator station, DCS controller) need to be carefully protected since they are directly responsible for controlling the end processes.

A. Edge clients
B. Typical IT system
C. ICSs and their real time OSs
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

107. ICSs can have very complex interactions with physical processes and consequences in the ICS domain can manifest in physical events. Which of the following terms is integrated into the industrial control system must be tested to prove that they do not compromise normal ICS functionality?

A. Current security capabilities
B. All security functions
C. More difficult to upgrade
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

108. In a typical IT system, access control can be implemented without significant regard for _____.

A. ICS experts
B. Typical IT system
C. Data flow
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

109. Which of the following terms are especially vulnerable to resource unavailability and timing disruptions?

A. Policies and procedures
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. Legacy systems
F. None of the Above

110. Which of the following terms are more difficult to upgrade in a control system network? Many systems may not have desired features including encryption capabilities, error logging, and password protection.

A. Current security capabilities
B. Software and hardware applications
C. More difficult to upgrade
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

111. ICSs and their real time OSs are often resource-constrained systems that typically do not include_____. There may not be computing resources obtainable on ICS components to retrofit these systems with current security capabilities.

A. ICS experts
B. Typical IT system
C. Typical IT security capabilities
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

112. Which of the following terms and media used by ICS environments for field device control and intra-processor communication are typically dissimilar from the generic IT environment, and may be proprietary?

A. Current security capabilities
B. Communication protocols
C. More difficult to upgrade
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

113. Change management is paramount to maintaining the integrity of _____.

A. ICS experts
B. Typical IT system
C. ICSs and their real time OSs
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

114. Which of the following terms represent one of the greatest vulnerabilities to a system?

A. Proprietary protocols
B. Third-party security solutions
C. OPC
D. Unpatched systems
E. WANs and the Internet
F. None of the Above

115. Which of the following terms on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policy and procedures. In addition, these procedures are often automated using server-based tools.

A. ICS experts
B. Software updates
C. ICSs and their real time OSs
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

116. Software updates on ICSs cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the vendor of the industrial control application and the end user of the application before being implemented and _____often must be planned and scheduled days/weeks in advance.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. ICS outages
E. Third-party cyber security solutions
F. None of the Above

117. The ICS may also require revalidation as part of the update process. Change management is also applicable to_____. The change management process, when applied to ICSs, requires careful assessment by ICS experts working in conjunction with security and IT personnel.

A. Hardware and firmware
B. Typical IT system
C. ICSs and their real time OSs
D. Both IT and control systems
E. Automated using server-based tools
F. None of the Above

118. Typical IT systems allow for diversified support styles, perhaps to support disparate but_____.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Lifetime of the deployed technology
E. interconnected technology architectures
F. None of the Above

119. Which of the following terms have a lifetime on the order of 3-5 years, with brevity due to the quick evolution of technology?

A. Proprietary protocols
B. Third-party security solutions
C. OPC
D. Defense-in-depth strategy for the ICS
E. Typical IT components
F. None of the Above

120. For ICSs where technology has been established in many cases for very specific use and implementation, the _____ is often in the order of 15-20 years and sometimes longer.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Lifetime of the deployed technology
E. Third-party cyber security solutions
F. None of the Above

121. Typical IT components are typically local and easy to access, while ICS components can be isolated, remote, and require _____.

A. ICS experts
B. Typical IT system
C. ICSs and their real time OSs
D. Both IT and control systems
E. Extensive physical effort to gain access to them
F. None of the Above

122. Obtainable computing resources for ICSs (including central processing unit [CPU] time and memory) tend to be very limited because these systems were designed to maximize control system resources, with little to no extra capacity for _____.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Lifetime of the deployed technology
E. Third-party cyber security solutions
F. None of the Above

123. In some instances, _____ are not allowed due to vendor license agreements and loss of service support can occur if third party applications are installed.

A. Proprietary protocols
B. Third-party security solutions
C. OPC
D. Defense-in-depth strategy for the ICS
E. WANs and the Internet
F. None of the Above

124. Which of the following terms can come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as from system complexities, human errors and accidents, equipment failures and natural disasters?

A. Policies and procedures
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. Threats to control systems
F. None of the Above

125. To protect against adversarial threats (as well as known natural threats), it is necessary to create a defense-in-depth strategy for the_____.

A. Proprietary protocols
B. ICS
C. OPC
D. Defense-in-depth strategy for the ICS
E. WANs and the Internet
F. None of the Above

126. The following lists vulnerabilities that may be found in typical ICSs. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. The vulnerabilities are grouped into _____ categories to assist in determining optimal mitigation strategies.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Policy and Procedure, Platform, and Network
E. Third-party cyber security solutions
F. None of the Above

127. ICS vendors have begun to open up their proprietary protocols and publish their protocol specifications to enable third-party manufacturers to build _____.

A. Proprietary protocols
B. Third-party security solutions
C. Compatible accessories
D. Defense-in-depth strategy for the ICS
E. WANs and the Internet
F. None of the Above

128. Organizations are also transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft Windows and Unix-like operating systems as well as common networking protocols such as TCP/IP to reduce costs and_____ .

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Lifetime of the deployed technology
E. Improve performance
F. None of the Above

129. Another standard contributing to this evolution of open systems is OPC, a protocol that enables interaction between control systems and _____.

A. Current security capabilities
B. Protection
C. PC-based application programs
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

130. The transition to using these open protocol standards provides economic and technical benefits, but also increases the susceptibility of ICSs to cyber incidents. These standardized protocols and technologies have _____, which are susceptible to sophisticated and effective exploitation tools that are widely obtainable and relatively easy to use.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. Lifetime of the deployed technology
E. Third-party cyber security solutions
F. None of the Above

131. In addition, corporate networks are often connected to strategic partner networks and to the Internet. Control systems also make more use of WANs and the Internet to transmit data to their _____.

A. Proprietary protocols
B. Third-party security solutions
C. OPC
D. Remote or local stations and individual devices
E. WANs and the Internet
F. None of the Above

132. This integration of control system networks with public and corporate networks increases the _____ .

A. Current security capabilities
B. Protection
C. More difficult to upgrade
D. Normal ICS functionality
E. Accessibility of control system vulnerabilities
F. None of the Above

133. Unless appropriate security controls are installed, these vulnerabilities can expose all levels of the ICS network architecture to complexity-induced error, adversaries and a variety of cyber threats, including _____.

A. Proprietary protocols
B. Third-party security solutions
C. Worms and other malware
D. Defense-in-depth strategy for the ICS
E. WANs and the Internet
F. None of the Above

134. Which of the following terms is designed to track incidents of a cyber security nature that directly affect ICSs and processes? This includes events such as accidental cyber-associated incidents, as well as deliberate events such as unauthorized remote access, DoS attacks, and malware infiltrations.

A. Optimal mitigation strategies
B. Common networking protocols
C. Commonly known vulnerabilities
D. An Industrial Security Incident Database (ISID)
E. Third-party cyber security solutions
F. None of the Above

135. Data is collected through investigation into _____and from private reporting by member organizations that wish to have access to the database.

A. Current security capabilities
B. Protection
C. Publicly known incidents
D. Normal ICS functionality
E. Especially vulnerable
F. None of the Above

136. Each incident is researched and _____ (confirmed, likely but unconfirmed, unlikely or unknown, and hoax/urban legend).

A. Proprietary protocols
B. Third-party security solutions
C. Then rated according to reliability
D. Defense-in-depth strategy for the ICS
E. WANs and the Internet
F. None of the Above

Topic 4- ICS Security Program Development Section

137. Organizations should develop and deploy an ICS security program.ICS security plans and programs should be regular with and integrated with_____, programs, and practices, but must be tailored to the detailed requirements and characteristics of ICS technologies and environments.

A. Economic impacts
B. Undesirable incidents
C. Existing IT security experience
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

138. Which of the following terms mandates that the threat to the ICS should be measured and monitored to protect the interests of employees, the public, shareholders, customers, vendors, and the larger society?

A. Policies and procedures
B. Responsible risk management
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

139. The importance of secure systems should be further highlighted as business reliance on _____.

A. Economic impacts
B. Undesirable incidents
C. Interconnectivity increases
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

140. DoS attacks and malware (e.g., worms, viruses) have become all too common and have already impacted ICSs. In addition, a cyber breach in some sectors can have _____.

A. Policies and procedures
B. The cyber security team
C. Significant physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

141. Physical impacts include the set of direct consequences of_____. The potential effects of paramount importance include personal injury and loss of life. Other effects include the loss of property (including data) and damage to the environment.

A. Economic impacts
B. Undesirable incidents
C. ICS failure
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

142. Economic impacts are a second-order effect from physical impacts resulting from _____ .

A. Policies and procedures
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. An ICS incident
F. None of the Above

143. Which of the following terms could result in consequences to system operations, which in turn inflict a greater economic loss on the facility or organization. On a larger scale, these effects could negatively impact the local, regional, national, or possibly global economy.

A. Policies and procedures
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

144. Another second-order effect, the repercussions from the loss of national or public confidence in an organization, is many times overlooked. It is, however, a very real target and one that could be accomplished through _____.

A. Economic impacts
B. Undesirable incidents
C. An ICS incident
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

145. Which of the following terms of any sort detract from the value of an enterprise, but safety and security incidents can have longer-term negative impacts than other types of incidents on all stakeholders—employees, shareholders, customers, and the communities in which an organization operates?

A. Undesirable incidents
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

146. Effectively integrating security into an ICS requires defining and executing a comprehensive program that addresses_____, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement.

A. Economic impacts
B. Undesirable incidents
C. All aspects of security
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

147. Cyber security programs with visible, top-level support from _____ are more likely to achieve compliance, function more smoothly, and have earlier success than programs that do not have that support.

A. Policies and procedures
B. The cyber security team
C. Physical impacts
D. Cyber security programs
E. Organization leaders
F. None of the Above

148. Whenever a new system is being planned and installed, it is imperative to take the time to address security throughout the lifecycle, from architecture to procurement to installation to _____.

A. Economic impacts
B. Undesirable incidents
C. Maintenance to decommissioning
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

149. There are serious risks in deploying systems to production based on the postulation that they will be secured later. If there are _____ to secure the system appropriately before deployment, it is unlikely that there will be sufficient time and resources later to address security.

A. Policies and procedures
B. Insufficient time and resources
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

150. While the control engineers will play a large role in securing the ICS, they will not be able to do so without teamwork and support from both the _____. IT often has years of security experience, much of which is applicable to ICS.

A. Economic impacts
B. Undesirable incidents
C. There are serious risks
D. ICS technologies and environments
E. IT department and management
F. None of the Above

151. The cyber security team should develop the corporate policy that defines the guiding charter of the security organization and the roles, responsibilities, and accountabilities of _____.

A. Policies and procedures
B. System owners and users
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

152. The cyber security team should agree upon and document the objective of the security program, the business organizations affected, all the computer systems and networks involved, the budget and resources required, and the division of responsibilities. The scope can also address business, training, audit, legal, and regulatory requirements, as well as _____.

A. Economic impacts
B. Undesirable incidents
C. Timetables and responsibilities
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

153. Policies and procedures are at the root of every successful security program and wherever possible, _____should be joined with existing operational/management policies.

A. Economic impacts
B. Undesirable incidents
C. ICS specific polices and procedures
D. ICS technologies and environments
E. Damage to the environment
F. None of the Above

154. Which of the following terms aid to ensure that security protection is both regular and current to protect against evolving threats, and also help to educate?

A. The security testing
B. Policies and procedures
C. Perform incorrect actions
D. Detailed risk assessment
E. The vulnerability assessment
F. None of the Above

155. After the risks for the various systems are clearly understood, the cyber security team should examine _____ to see if they sufficiently address the risks to the ICS.

A. Policies and procedures
B. Existing security policies
C. Physical impacts
D. Cyber security programs
E. DoS attacks and malware
F. None of the Above

156. Security procedures should be documented, tested, and updated periodically in response to policy and technology changes. Consider developing ICS security policies and procedures based on the_____, deploying progressively heightened security postures as the Threat Level increases.

A. Economic impacts
B. Undesirable incidents
C. There are serious risks
D. ICS technologies and environments
E. Homeland Security Advisory System Threat Level
F. None of the Above

157. The cyber security team ought to identify the applications and computer systems within the ICS, as well as the networks within and interfacing to the ICS. The focus should be on systems rather than just devices, and should include _____ and instrument-based systems that use a monitoring device such as an HMI.

A. Detailed vulnerability assessment
B. PLCs, DCSs, SCADA
C. Any problems that arise
D. Identifying the vulnerabilities
E. Attempt to verify vulnerabilities
F. None of the Above

158. There are several commercial enterprise inventory tools that can identify and document all hardware and software resident on a network. Care must be taken before using these tools to locate ICS assets; teams should first conduct an assessment of how these tools work and what impact they might have on the_____.

A. Security testing
B. Connected control equipment
C. Perform incorrect actions
D. Detailed risk assessment
E. The vulnerability assessment
F. None of the Above

159. The organization should then implement a detailed vulnerability assessment for the highest-priority systems and assessments for _____as deemed prudent/as resources allow.

A. Detailed vulnerability assessment
B. Lower-priority systems
C. Any problems that arise
D. Identifying the vulnerabilities
E. Attempt to verify vulnerabilities
F. None of the Above

160. Which of the following terms will help identify any weaknesses that may be present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the associated cyber security risks and mitigation approaches to reduce the risks?

A. The security testing
B. Time-critical assessment
C. Implement incorrect actions
D. Detailed risk assessment
E. The vulnerability assessment
F. None of the Above

161. Vulnerability scanners often attempt to confirm vulnerabilities by _____ and conducting a representative set of attacks against devices and networks.

A. Detailed vulnerability assessment
B. Extensively probing
C. Any problems that arise
D. Identifying the vulnerabilities
E. Attempt vulnerabilities
F. None of the Above

162. ICSs were planned and built to control and automate real-world processes or _____. Given the wrong instructions, they could implement incorrect actions, causing waste, equipment damage, injury, or even deaths.

A. The security testing
B. Equipment
C. Implement incorrect actions
D. Detailed risk assessment
E. The vulnerability assessment
F. None of the Above

163. Recognizing the vulnerabilities within an ICS requires a dissimilar approach than in a typical IT system. In most cases, devices on an IT system can be rebooted, restored, or replaced with _____ .

A. Detailed vulnerability assessment
B. Little interruption of service to its customers
C. Any problems that arise
D. Identifying the vulnerabilities
E. Attempt to verify vulnerabilities
F. None of the Above

164. An ICS controls a physical process and therefore has real-world consequences associated with its actions. Some actions are time-critical, while others have a _____.

A. Security testing
B. More relaxed timeframe
C. Perform incorrect actions
D. Detailed risk assessment
E. Vulnerability assessment
F. None of the Above

165. When any assessment of an ICS is being implemented, ICS personnel must be aware that testing is occurring, and be prepared to immediately tackle _____.

A. Detailed vulnerability assessment
B. PLCs, DCSs, SCADA
C. Any problems that arise
D. Identifying the vulnerabilities
E. Attempt to verify vulnerabilities
F. None of the Above

166. If manual control of the system is possible, personnel capable of implementing manual control should be present during the _____.

A. Security testing
B. Time-critical
C. Perform incorrect actions
D. Detailed risk assessment
E. The vulnerability assessment
F. None of the Above

167. Additionally, security auditors need to understand the ICS under test, the risk involved with the test, and the consequences associated with unintentional stimulus or_____ .

A. Detailed vulnerability assessment
B. PLCs, DCSs, SCADA
C. Any problems that arise
D. Identifying the vulnerabilities
E. DoS to the ICS
F. None of the Above

168. Organizations should understand the detailed risk assessment, identify the cost of mitigation for each risk, compare the cost with the_____, and select those mitigation controls where cost is less than the potential risk.

A. Security testing
B. Risk of occurrence
C. Perform incorrect actions
D. Detailed risk assessment
E. Vulnerability assessment
F. None of the Above

169. The controls to mitigate a detailed risk may vary among types of systems. For example, _____ might be dissimilar for ICSs than for corporate payroll systems and e-commerce systems.

A. Other security sensors
B. Other possible deployments
C. Initiate response to cyber incidents
D. User authentication controls
E. Firewalls used to protect control systems
F. None of the Above

170. Implementing _____ may bring changes to the way in which personnel access computer programs, applications, and the computer desktop itself.

A. Redundant access points
B. Hardware firewalls
C. An ICS security program
D. Management of firewall configurations
E. Blocking
F. None of the Above

Topic 5- Network Architecture Section

171. When designing a network architecture for an ICS deployment, it is typically recommended to separate the ICS network from the corporate network. The nature of network traffic on these two networks is dissimilar: Internet access, FTP, e-mail, and remote access will typically be permitted on the _____ but should not be on the ICS network.

A. A firewall and a DMZ
B. Network environments
C. ICS network
D. Corporate network
E. Dedicated hardware firewalls
F. None of the Above

172. Rigorous change control procedures for_____ , configuration, and software changes may not be in place on the corporate network.

A. High level of security
B. Network firewall(s)
C. Data from the ICS
D. Network equipment
E. Corporate network
F. None of the Above

173. If ICS network traffic is carried on the corporate network, it could be intercepted or be subjected to a denial of service attack. By having separate networks, _____ on the corporate network should not be able to affect the ICS network.

A. A firewall and a DMZ
B. Network environments
C. Security and performance problems
D. Stateful inspection firewalls filter packets
E. Dedicated hardware firewalls
F. None of the Above

174. Practical contemplations often mean that a connection is required between the ICS and corporate networks. This connection is _____ and careful consideration should be given to the design.

A. High level of security
B. Network firewall(s)
C. Data from the ICS
D. A significant security risk
E. Corporate network
F. None of the Above

175. If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through _____.

A. A firewall and a DMZ
B. Network environments
C. ICS network
D. Stateful inspection firewalls filter packets
E. Dedicated hardware firewalls
F. None of the Above

176. A DMZ is a separate network segment that connects directly to _____. Servers containing the data from the ICS that needs to be accessed from the corporate network are put on this network segment.
A. High level of security D. The firewall
B. Network firewall(s) E. Corporate network
C. Data from the ICS F. None of the Above

177. Only DMZ systems should be accessible from the corporate network. With any external connections, the minimum access should be permitted through the firewall, including _____.
A. A firewall and a DMZ D. Opening only the ports required for specific communication
B. Network environments E. Dedicated hardware firewalls
C. ICS network F. None of the Above

178. Network firewalls are devices or systems that control the flow of network traffic between networks engaging differing _____.
A. Security postures D. A significant security risk
B. Network firewall(s) E. Corporate network
C. Data from the ICS F. None of the Above

179. Firewalls have applicability in _____ that do not include or require Internet connectivity.
A. A firewall and a DMZ D. Stateful inspection firewalls filter packets
B. Network environments E. Dedicated hardware firewalls
C. ICS network F. None of the Above

180. By engaging firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within_____ .
A. High level of security D. A significant security risk
B. The more sensitive areas E. Corporate network
C. Data from the ICS F. None of the Above

181. Which of the following terms at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the transport layer (e.g., TCP, UDP) as well?
A. A firewall and a DMZ packets D. Stateful inspection firewalls filter packets
B. Network environments packets E. Dedicated hardware firewalls packets
C. ICS network packets F. None of the Above

182. Which of the following terms keeps track of active sessions and uses that information to determine if packets should be forwarded or blocked? It offers a high level of security and good performance, but it may be more expensive and complex to administer. Additional rule sets for ICS applications may be required.
A. High level of security D. A significant security risk
B. Network firewall(s) E. Stateful inspection
C. Data from the ICS F. None of the Above

183. In an ICS environment, _____are most often installed between the ICS network and the corporate network.

A. A firewall and a DMZ
B. Network environments
C. ICS network
D. Firewalls
E. Dedicated hardware firewalls
F. None of the Above

184. Appropriately configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security. They can also potentially improve a control network's responsiveness by removing _____.

A. High level of security
B. Network firewall(s)
C. Data from the ICS
D. A significant security risk
E. Non-essential traffic from the network
F. None of the Above

185. When designed, configured, and maintained appropriately, dedicated hardware firewalls can contribute significantly to increasing the_____.

A. Firewall and a DMZ
B. Network environments
C. ICS network
D. Security of today's ICS environments
E. Dedicated hardware firewalls
F. None of the Above

186. Firewalls provide several tools to enforce a security policy that cannot be accomplished locally on the current set of process control devices obtainable in the market, including the ability to: Block all communications with the exception of definitive enabled communications between devices on the _____.

A. High level of security
B. Network firewall(s)
C. Data from the ICS
D. Unprotected LAN and protected ICS networks
E. Corporate networks
F. None of the Above

187. Blocking is based on source and_____.

A. Other security sensors
B. Other possible deployments
C. Initiate response
D. Destination IP address pairs, services, and ports
E. Firewalls used to protect control systems
F. None of the Above

188. Blocking can occur on _____ , which is helpful in limiting high-risk communications such as e-mail.

A. Redundant access points
B. Hardware firewalls
C. Users can be restricted
D. Management of firewall configurations
E. Both inbound and outbound packets
F. None of the Above

189. Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, two-factor authentication technologies, tokens, biometrics and smart cards. Select the particular method based upon the _____ to be protected, rather than using the method that is obtainable at the device level.

A. Other security sensors
B. Other possible deployments
C. Vulnerability of the ICS network
D. Enforce secure authentication
E. Firewalls used to protect control systems
F. None of the Above

190. Enforce destination authorization. _____ can be limited and allowed to reach only the nodes on the control network necessary for their job function. This reduces the potential of users intentionally or accidentally gaining access to and control of devices for which they are not authorized, but adds to the complexity for on-the-job-training or cross-training employees.

A. Redundant access points
B. Hardware firewalls
C. Users
D. Management of firewall configurations
E. Blocking
F. None of the Above

191. Other possible deployments include using either _____ or small standalone hardware firewalls in front of, or running on, individual control devices.

A. Other security sensors
B. Other possible deployments
C. Host-based firewalls
D. Enforce secure authentication
E. Firewalls used to protect control systems
F. None of the Above

192. Using firewalls on an individual device basis can create substantial management overhead, especially in change management of _____.

A. Redundant access points
B. Hardware firewalls
C. Users can be restricted
D. Firewall configurations
E. Blocking
F. None of the Above

193. There are several issues that must be addressed when deploying firewalls in ICS environments, particularly the following: Firewalls used to protect control systems should be configured so they do not permit either incoming or outgoing traffic by default. The default configuration should only be modified when it is necessary to _____.

A. Other security sensors
B. Other possible deployments
C. Initiate response to cyber incidents
D. Enforce secure authentication
E. Permit connections to or from trusted systems
F. None of the Above

194. Which of the following terms do require ongoing support, maintenance, and backup? Rule sets need to be reviewed to make sure that they are providing adequate protection in light of ever-changing security threats.

A. Redundant access points
B. Hardware firewalls
C. Users can be restricted
D. Management of firewall configurations
E. Blocking
F. None of the Above

195. System capabilities, such as available disk space, should be monitored to make sure that the firewall is achieving its data collection tasks and can be depended upon in the event of a _____.

A. Other security sensors
B. Other possible deployments
C. Initiate response to cyber incidents
D. Enforce secure authentication
E. Security violation
F. None of the Above

196. Real-time monitoring of firewalls and other security sensors is required to rapidly detect and initiate response to _____.

A. Other security sensors
B. Other possible deployments
C. Cyber incidents
D. Enforce secure authentication
E. Firewalls used to protect control systems
F. None of the Above

197. The ICS network should, at a minimum, be logically separated from the corporate network on _____ . When enterprise connectivity is required: There should be documented and minimal (single if possible) access points between the ICS network and the corporate network. Redundant access points, if present, must be documented.

A. Redundant access points
B. Hardware firewalls
C. Users can be restricted
D. Management of firewall configurations
E. Physically separate network devices
F. None of the Above

198. A stateful firewall between the ICS network and _____ should be configured to deny all traffic except that which is explicitly authorized.

A. Other security sensors
B. Other possible deployments
C. Initiate response to cyber incidents
D. Enforce secure authentication
E. Corporate network
F. None of the Above

199. The firewall rules should at a minimum provide source and destination filtering (i.e. filter on media access control [MAC] address), in addition to TCP and User Datagram Protocol (UDP) port filtering and ICMP type and _____.

A. Redundant access points
B. Code filtering
C. Users can be limited
D. Management of firewall configurations
E. Blocking
F. None of the Above

200. An acceptable approach to enabling communication between _____ and a corporate network is to implement an intermediate DMZ network.

A. Other security sensors
B. Other possible deployments
C. Initiate response to cyber incidents
D. Enforce secure authentication
E. An ICS network
F. None of the Above

201. The DMZ should be connected to the _____such that detailed (limited) communication may occur between only the corporate network and the DMZ, and the ICS network and the DMZ.

A. Redundant access points
B. Hardware firewalls
C. Firewall
D. Management of firewall configurations
E. Blocking
F. None of the Above

202. The corporate network and the _____ should not communicate directly with each other.

A. DMZ
B. DMZ-capable firewall
C. An antivirus server
D. ICS network
E. The primary security risk
F. None of the Above

203. ICS networks and corporate networks can be segregated to enhance cyber security using_____ .

A. Each DMZ
B. Historian's application layer code
C. Different architectures
D. Wireless access points on the DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

204. If the _____resides on the control network, a firewall rule must exist that allows all hosts from the enterprise to communicate with the historian. Typically, this communication occurs at the application layer as Structured Query Language (SQL) or HTTP requests.

A. DMZ
B. DMZ-capable firewall
C. Antivirus server
D. Data historian
E. Primary security risk
F. None of the Above

205. Flaws in the historian's application layer code could result in a compromised historian. Once the historian is compromised, the remaining nodes on the _____are vulnerable to a worm propagating or an interactive attack.

A. Each DMZ
B. Control network
C. ICS network
D. Wireless access points on the DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

206. A substantial improvement is the use of firewalls with the ability to establish a _____.

A. DMZ
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. DMZ between the corporate and control networks
F. None of the Above

207. Which of the following terms holds one or more critical components, such as the data historian, the wireless access point, or remote and third party access systems?

A. Each DMZ
B. Historian's application layer code
C. ICS network
D. Wireless access points on the DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

208. In effect, the use of a DMZ-capable firewall allows the creation of _____.

A. DMZ
B. An intermediate network
C. An antivirus server
D. The corporate network and the ICS network
E. The primary security risk
F. None of the Above

209. Creating a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces. One of the interfaces is connected to the corporate network, the second to the control network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points on the _____.

A. Each DMZ
B. Historian's application layer code
C. ICS network
D. DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

Patch Management Server

210. By placing corporate-accessible components in the DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the _____.

A. DMZ
B. DMZ-capable firewall
C. Antivirus server
D. Corporate network and the ICS network
E. Primary security risk
F. None of the Above

211. Most firewalls can allow for_____ , and can specify what type of traffic may be forwarded between zones.

A. Multiple DMZs
B. Historian's application layer code
C. ICS network
D. Wireless access points on the DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

212. If a patch management server, an antivirus server, or other security server is to be used for the control network, it should be located directly on the DMZ. Both functions could reside on a _____.

A. Single server
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. The primary security risk
F. None of the Above

213. Having patch management and antivirus management dedicated to the control network allows for controlled and secure updates that can be tailored for the unique needs of the ICS environment. It may also helpful if the antivirus product chosen for ICS protection is not the same as the antivirus product used for the _____.

A. Each DMZ
B. Corporate network
C. ICS network
D. Wireless access points on the DMZ network
E. DMZ between the corporate and control networks
F. None of the Above

214. The primary security risk in this type of architecture is that if a computer in the DMZ is compromised, then it can be used to launch an attack against the control network via application traffic permitted from _____.

A. The DMZ to the control network
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. The primary security risk
F. None of the Above

215. In summary, non-firewall-based solutions will generally not provide suitable isolation between control networks and corporate networks. _____ are marginally acceptable but should be only be installed with extreme care.

A. DMZ
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. The two-zone solutions (no DMZ)
F. None of the Above

216. The most secure, manageable, and _____and corporate network segregation architectures are typically based on a system with at least three zones, incorporating a DMZ.

A. Corporate network
B. DMZ
C. Scalable control network
D. Control network
E. A defense-in-depth architecture
F. None of the Above

217. A single security product, technology or solution cannot adequately protect _____ by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms, a technique also known as defense-in-depth, is desired so that the impact of a failure in any one mechanism is minimized.

A. An ICS
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. The primary security risk
F. None of the Above

218. A defense-in-depth architecture strategy includes the use of firewalls, the creation demilitarized zones, _____along with effective security policies, training programs and incident response mechanisms.

A. Corporate network
B. DMZ
C. Intrusion detection capabilities
D. Control network
E. A defense-in-depth architecture
F. None of the Above

219. When installing a _____ without a DMZ for shared servers, particular care needs to be taken with the rule design.

A. Single two-port firewall
B. DMZ-capable firewall
C. An antivirus server
D. The corporate network and the ICS network
E. The primary security risk
F. None of the Above

220. At a minimum, all rules should be stateful rules that are both IP address and port (application) specific. The address portion of the rules should restrict incoming traffic to a very small set of shared devices (e.g., the data historian) on the control network from a controlled set of addresses on the _____.

A. Corporate network
B. DMZ
C. Allowed ports
D. Control network
E. A defense-in-depth architecture
F. None of the Above

221. Allowing any IP addresses on the _____ to access servers inside the control network is not recommended.

A. Corporate network
B. DMZ
C. Allowed ports
D. Control network
E. A defense-in-depth architecture
F. None of the Above

222. In addition, _____should be carefully limited to relatively secure protocols such as Hypertext Transfer Protocol Secure (HTTPS).

A. Corporate network
B. DMZ
C. The allowed ports
D. Control network
E. A defense-in-depth architecture
F. None of the Above

223. Allowing HTTP, FTP, or any unencrypted SCADA protocol to cross the _____is a security risk due to the potential for traffic sniffing and modification.

A. Control networks
B. Firewall
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

224. Rules should be added to deny inbound communication with the_____.

A. Corporate network
B. DMZ
C. Allowed ports
D. Control network
E. A defense-in-depth architecture
F. None of the Above

225. Rules should only allow devices internal to the _____ the ability to establish connections outside the control network.

A. Control networks
B. Correct source IP address
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

226. On the other hand, if the _____is being used, then it is possible to configure the system so that no traffic will go directly between the corporate network and the control network. With a few special exceptions (noted below), all traffic from either side can terminate at the servers in the DMZ. This allows more flexibility in the protocols allowed through the firewall.

A. Corporate network
B. DMZ
C. DMZ architecture
D. Control network
E. Defense-in-depth architecture
F. None of the Above

227. Which of the following terms might be used to communicate from the PLCs to the data historian, while HTTP might be used for communication between the historian and enterprise clients?

A. PLCs
B. Rules
C. DoS attacks
D. MODBUS/TCP
E. Ports and services
F. None of the Above

228. Both protocols are inherently insecure, yet in this case, they can be used safely because neither actually crosses between the_____ .

A. Two networks
B. Correct source IP address
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

229. An extension to this concept is the idea of using "disjoint" protocols in all control network to corporate network communications. That is, if a protocol is allowed between the _____, then it is explicitly **not** allowed between the DMZ and corporate network.

A. PLCs
B. Control network and DMZ
C. DoS attacks
D. DMZ and corporate network
E. Ports and services
F. None of the Above

230. In addition to these rules, the firewall should be configured with outbound filtering to stop forged IP packets from leaving the _____ . In practice this is achieved by checking the source IP addresses of outgoing packets against the firewall's respective network interface address.

A. Control networks
B. Correct source IP address
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Control network or the DMZ
F. None of the Above

231. The intent is to prevent the control network from being the source of spoofed (i.e., forged) communications, which are often used in DoS attacks. Thus, the firewalls should be configured to forward IP packets only if those packets have a correct source IP address for the _____ .

A. Control network or DMZ networks
B. Rules
C. DoS attacks
D. DMZ and corporate network
E. Ports and services
F. None of the Above

Summary

232. In summary, the following should be considered as recommended practice for general firewall rule sets: The base rule set should be deny all, permit none. _____ between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis.

A. Control networks
B. Correct source IP address
C. Ports and services
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

233. There should be a documented business justification with risk analysis and a responsible person for each_____ .

A. PLCs
B. Rules
C. DoS attacks
D. Permitted incoming or outgoing data flow
E. Ports and services
F. None of the Above

234. All "permit" rules should be both IP address and_____, and stateful if appropriate.

A. Control networks
B. Correct source IP address
C. TCP/UDP port specific
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

235. All rules should restrict traffic to _____ or range of addresses.

A. A specific IP address
B. Rules
C. DoS attacks
D. DMZ and corporate network
E. Ports and services
F. None of the Above

236. Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the_____.

A. Control networks
B. Correct source IP address
C. DMZ
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

237. Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and _____(and vice-versa).

A. Control networks
B. Corporate networks
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

238. All outbound traffic from the control network to the corporate network should be source and _____ .

A. PLCs
B. Rules
C. DoS attacks
D. DMZ and corporate network
E. Destination-restricted by service and port
F. None of the Above

239. Outbound packets from the control network or DMZ should be allowed only if those packets have _____ that is assigned to the control network or DMZ devices.

A. Control networks
B. Correct source IP address
C. A correct source IP address
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

240. Control network devices should not be allowed to access _____.
A. PLCs
B. The Internet
C. DoS attacks
D. DMZ and corporate network
E. Ports and services
F. None of the Above

241. Which of the following terms should not be directly connected to the Internet, even if protected via a firewall?
A. Control networks
B. Correct source IP address
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

242. All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with two-factor authentication. Traffic should also be limited by IP address to _____.
A. PLCs
B. Specific management stations
C. DoS attacks
D. DMZ and corporate network
E. Ports and services
F. None of the Above

243. Which of the following terms are used for transferring files between devices? They are implemented on almost every platform including many SCADA systems, DCSs, PLCs, and RTUs, since they are very well known and use minimum processing power.
A. Control networks
B. Correct source IP address
C. Traffic
D. FTP and Trivial File Transfer Protocol (TFTP)
E. Both IP address and TCP/UDP port specific
F. None of the Above

244. Neither protocol was created with security in mind; for_____, the login password is not encrypted, and for TFTP, no login is required at all.
A. FTP
B. All TFTP communications
C. DoS attacks
D. DMZ and corporate network
E. Security controls
F. None of the Above

245. Some FTP implementations have a history of buffer overflow vulnerabilities. As a result, _____ should be blocked, while FTP communications should be allowed for outbound sessions only or if secured with additional token-based two-factor authentication and an encrypted tunnel. More secure protocols, such as Secure Copy (SCP), should be employed whenever possible.
A. FTP
B. All TFTP communications
C. DoS attacks
D. DMZ and corporate network
E. Security controls
F. None of the Above

Topic 6 – ICS Security Controls Section

246. Which of the following missing terms are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information?
A. FTP
B. All TFTP communications
C. DoS attacks
D. DMZ and corporate network
E. Security controls
F. None of the Above

247. Which of the following missing terms are organized into three classes; management, operational, and technical controls?

A. FTP
B. All TFTP communications
C. DoS attacks
D. DMZ and corporate network
E. Security controls
F. None of the Above

248. Each class is broken into several families of controls; each control contains a definition of the control, supplemental guidance, and _____that will increase the strength of a basic control.

A. Responding to incidents
B. Impact of a failure
C. Protect the confidentiality
D. Producing the desired outcome
E. Possible enhancements
F. None of the Above

249. A single security product or technology cannot adequately protect an ICS. Securing an ICS is based on _____ and an appropriately configured set of security controls.

A. Identifying risks to operations
B. Allocation of resources
C. A risk assessment
D. Prioritization of vulnerabilities
E. A combination of effective security policies
F. None of the Above

250. An effective cyber security strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized.

A. Responding to incidents
B. Impact of a failure
C. Protect the confidentiality
D. Producing the desired outcome
E. Will increase the strength
F. None of the Above

Management Controls

251. Management controls are the security countermeasures for an ICS that focus on the management of risk and the management of information security. NIST SP 800-53 defines four families of controls within the Management controls class: Risk Assessment (RA): the process of identifying risks to_____ by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact

A. Identifying risks to operations
B. Allocation of resources
C. A risk assessment
D. Operations, assets, or individuals
E. Impact of exploiting this vulnerability
F. None of the Above

252. Planning (PL): development and maintenance of a plan to address information system security by executing assessments, specifying and implementing security controls, assigning security levels, and _____.

A. Responding to incidents
B. Impact of a failure
C. Protect the confidentiality
D. Producing the desired outcome
E. Will increase the strength
F. None of the Above

253. System and Services Acquisition (SA): allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on _____ including requirements, design criteria, test procedures, and associated documentation.

A. Identifying risks to operations
B. Risk assessment results
C. A risk assessment
D. Prioritization of vulnerabilities
E. Impact of exploiting this vulnerability
F. None of the Above

254. Certification, Accreditation, and Security Assessments (CA): assurance that the specified controls are implemented correctly, operating as intended, and _____.
A. Responding to incidents D. Producing the desired outcome
B. Impact of a failure E. Will increase the strength
C. Protect the confidentiality F. None of the Above

255. Risk is a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting _____.
A. Identifying risks to operations D. Prioritization of vulnerabilities
B. Allocation of resources E. Impact of exploiting this vulnerability
C. A risk assessment F. None of the Above

256. Which of the following terms is the process of identifying risks to an organization's operations, assets, and individuals by determining the probability of occurrence that an identified threat will exploit an identified vulnerability and the resulting impact?
A. Responding to incidents D. Producing the desired outcome
B. Impact of a failure E. Risk assessment
C. Protect the confidentiality F. None of the Above

257. An assessment includes _____ that can mitigate each threat and the costs associated with implementing them.
A. Identifying risks to operations D. Prioritization of vulnerabilities
B. An evaluation of security controls E. Impact of exploiting this vulnerability
C. A risk assessment F. None of the Above

258. Which of the following terms must also compare the cost of security with the costs associated with an incident?
A. Identifying risks to operations D. Prioritization of vulnerabilities
B. Allocation of resources E. impact of exploiting this vulnerability
C. A risk assessment F. None of the Above

259. Achieving an acceptable level of risk is a process of reducing the probability of an incident that is accomplished by _____ that can be exploited as well as consequences resulting from an incident.
A. Responding to incidents D. Producing the desired outcome
B. Impact of a failure E. Mitigating or eliminating vulnerabilities
C. Protect the confidentiality F. None of the Above

260. Which of the following terms must be based on cost and benefit with an objective to provide a business case for implementing at least a minimum set of control system security requirements to reduce risk to an acceptable level?
A. Identifying risks to operations D. Prioritization of vulnerabilities
B. Allocation of resources E. Impact of exploiting this vulnerability
C. A risk assessment F. None of the Above

261. A mistake often made during a risk assessment is to select technically interesting vulnerabilities without taking into account the_____. Vulnerabilities should be assessed and rated for risk before trying to select and implement security controls on them.
A. Responding to incidents D. Producing the desired outcome
B. Impact of a failure E. Level of risk associated with them
C. Protect the confidentiality F. None of the Above

Identify the missing term.
262. Produces a list of the system vulnerabilities that could be exercised by the potential threat sources
A. Impact analysis D. Results documentation
B. Likelihood determination E. Risk determination
C. Vulnerability identification F. None of the Above

263. Produces a list of the planned controls used for the information system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
A. Threat identification D. Vulnerability identification
B. Control recommendations E. Control analysis
C. System characterization F. None of the Above

264. Produces a likelihood rating (High, Medium, or Low) that indicates the probability that a potential vulnerability may be exercised
A. Impact analysis D. Results documentation
B. Likelihood determination E. Risk determination
C. Vulnerability identification F. None of the Above

265. Produces a picture of the information system environment, and delineation of system boundaries
A. Threat identification D. Vulnerability identification
B. Control recommendations E. Control analysis
C. System characterization F. None of the Above

266. Produces measurement for risk based on a scale of high, medium, or low.
A. Impact analysis D. Results documentation
B. Likelihood determination E. Risk determination
C. Vulnerability identification F. None of the Above

267. Produces recommendations of security controls and alternative solutions to mitigate risk
A. Threat identification D. Vulnerability identification
B. Control recommendations E. Control analysis
C. System characterization F. None of the Above

268. Produces a risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.
A. Impact analysis D. Results documentation
B. Likelihood determination E. Risk determination
C. Vulnerability identification F. None of the Above

269. Produces a threat statement containing a list of threat-sources that could exploit system vulnerabilities

A. Threat identification
B. Control recommendations
C. System characterization
D. Vulnerability identification
E. Control analysis
F. None of the Above

270. Produces a magnitude of impact (High, Medium, or Low) resulting from the exploitation of a vulnerability.

A. Impact analysis
B. Likelihood determination
C. Vulnerability identification
D. Results documentation
E. Risk determination
F. None of the Above

6.2 Operational Controls – Identify the statement.

271. Operational controls are the security countermeasures for an ICS that are primarily implemented and executed by people as opposed to systems. NIST SP 800-53 defines nine families of controls within the Operational controls class: _____ Policy and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.

A. Maintenance (MA)
B. Contingency Planning (CP)
C. Incident Response (IR)
D. Media Protection (MP)
E. Physical and Environmental Protection (PE)
F. None of the Above

272. Policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.

A. Configuration Management (CM)
B. Awareness and Training (AT)
C. Personnel Security (PS)
D. System and Information Integrity (SI)
E. Maintenance (MA)
F. None of the Above

273. Policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

A. Maintenance (MA)
B. Contingency Planning (CP)
C. Incident Response (IR)
D. Media Protection (MP)
E. Physical and Environmental Protection (PE)
F. None of the Above

274. Policy and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.

A. Configuration Management (CM)
B. Awareness and Training (AT)
C. Personnel Security (PS)
D. System and Information Integrity (SI)
E. Maintenance (MA)
F. None of the Above

275. Policy addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).

A. Maintenance (MA)
B. Contingency Planning (CP)
C. Incident Response (IR)
D. Media Protection (MP)
E. Physical and Environmental Protection (PE)
F. None of the Above

276. Policy and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls.

A. Configuration Management (CM)
B. Awareness and Training (AT)
C. Personnel Security (PS)
D. System and Information Integrity (SI)
E. Maintenance (MA)
F. None of the Above

277. Policy and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.

A. Maintenance (MA)
B. Contingency Planning (CP)
C. Incident Response (IR)
D. Media Protection (MP)
E. Physical and Environmental Protection (PE)
F. None of the Above

278. Policy and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

A. Configuration Management (CM)
B. Awareness and Training (AT)
C. Personnel Security (PS)
D. System and Information Integrity (SI)
E. Maintenance (MA)
F. None of the Above

279. Policies and procedures to manage all maintenance aspects of an information system.

A. Maintenance (MA)
B. Contingency Planning (CP)
C. Incident Response (IR)
D. Media Protection (MP)
E. Physical and Environmental Protection (PE)
F. None of the Above

Identify the missing term

280. The physical protection of the cyber components and data associated with the ICS must be addressed as part of the _____.

A. Overall security of a plant
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

281. Security at many ICS facilities is intimately tied to plant safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out _____.

A. Asset location technologies
B. Emergency procedures
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

282. Gaining physical access to a control room or control system components often implies gaining logical access to the _____ as well.

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Granted access
E. A secured area
F. None of the Above

283. If computers are readily accessible, and they have removable media drives (e.g., floppy disks, compact discs, etc.) or USB ports, the drives can be fitted with locks or removed from the computers and _____.

A. Asset location technologies
B. Access limiting systems
C. USB ports disabled
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

284. Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent _____.

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Granted access
E. A secured area
F. None of the Above

285. For maximum security, _____should be placed in locked areas and authentication mechanisms (such as keys) protected.

A. PLCs
B. Control network and DMZ
C. ICS network
D. DMZ and corporate network
E. Servers
F. None of the Above

286. The network devices on the _____, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

A. PLCs
B. Control network and DMZ
C. ICS network
D. DMZ and corporate network
E. Servers
F. None of the Above

287. Classic physical security contemplations typically refer to a _____of layered security measures.

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Ringed architecture
E. Classic physical security considerations
F. None of the Above

288. Creating several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or_____ , establishes these physical security perimeters.

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Granted access
E. Other informational assets
F. None of the Above

289. Access control systems should ensure that only authorized people have _____ .

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Access to controlled spaces
E. Classic physical security considerations
F. None of the Above

290. A system must be able to _____ are who they say they are (typically using something the person has, such as an access card; something they know, such as a personal identification number (PIN); or something they are, using abiometric).

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Verify that persons being granted access
E. A secured area
F. None of the Above

291. _____ should be highly reliable yet not interfere with the routine or emergency duties of plant personnel.

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Access control
F. None of the Above

292. Which of the following terms into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity?

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

293. Within an area, _____to network and computer cabinets should be limited to only those who have a need, such as network technicians and engineers, or computer maintenance staff.

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Access
E. Classic physical security considerations
F. None of the Above

294. Equipment cabinets should be locked and wiring should be neat and within cabinets. Consider keeping all computers in secure racks and using _____ to connect human-machine interfaces to the racked computers.

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

295. Which of the following terms include still and video cameras, sensors, and various types of identification systems?

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Access monitoring systems
F. None of the Above

296. Which of the following terms may employ a combination of devices to physically control or prevent access to protected resources.

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security considerations
F. None of the Above

297. Locating people and vehicles in a large installation is important for safety reasons, and it is _____ as well.

A. Overall security of a plant
B. Process control system
C. Unauthorized use
D. Increasingly important for security reasons
E. A secured area
F. None of the Above

298. Which of the following terms can be used to track the movements of people and vehicles within the plant, to ensure that they stay in authorized areas, to identify personnel needing assistance, and to support emergency response?

A. Asset location technologies
B. Access limiting systems
C. Peripheral extender technology
D. Integration of access control
E. Classic physical security contemplations
F. None of the Above

299. An alarm to the process control system should be generated when environmental specifications such as _____ are exceeded.

A. Threat identification
B. Temperature and humidity
C. System characterization
D. Vulnerability identification
E. Control analysis
F. None of the Above

300. Computers and computerized devices used for ICS functions (such as PLC programming) should never leave the_____. Laptops and portable engineering workstations should be tightly secured and never used outside the ICS network. Antivirus and patch management should be kept current.

A. Proprietary area
B. ICS area
C. OPC area
D. Defense strategy for the ICS
E. WAN area
F. None of the Above