Student ID	Tutorial participation Grade (5)	Coursework Grade (35)	Comments
RA6804071	3	5+6+6+3 =20 Total = 23/40	• Question 1 Cheating from BN0570273 • Question 2 Part a 1) Leakage detection in the tank using Sensor s6 is not considered in the ladder logic. 2) Leakage and blockage detection in the pipe using Sensor s2 and s3 are not considered in the ladder logic. 3) The ladder logic is designed in a wrong way, as the motor will be reset when there is water in the pipe. • Question 2 part b 1) The analysis of the attack does not consider the IT domain (the two stages of the Cyber Kill Chain should be considered). • Question 2 part C 1) Possible to write more on mitigations. The answer to Question 1 is good but, since it is shared with others, the mark is capped at 50%. The ladder logic is a reasonable attempt but has a few problems as indicated. You could have looked at ICS SERT Advisories to find mitigations that were more specific to this particular vulnerability.
BN0570273	1	5+6+6+5 = 22 Total = 23/40	• Question 1 Cheating from RA6804071 • Question 2 Part a 1) True value means the sensors should give 1 not 0 and false value means the sensors should give 0 not 1. 2) The ladder logic is designed in a wrong way, as the motor will be reset when there is water in the pipe. 3) s1 and s2 are pressure sensors which shouldn't have the same value before and after the pump. Otherwise, the pump will not work. • Question 2 part b 1) The analysis of the attack does not consider the IT domain (the two stages of the Cyber Kill Chain should be considered). The answer to Question 1 is good but, since it is shared with others, the mark is capped at 50%. The ladder logic is a reasonable attempt but has a few problems as indicated. The discussion of mitigations is fine.
904943	2	6+5+4+3 =18 Total = 20/40	• Question 1 Not clear at all! • Question 2 Part a 1) There is no sensor called P1 2) Each of these ladders is either incorrect or incomplete.

			• Question 2 part b 1) The analysis of the attack does not consider the IT domain (the two stages of the Cyber Kill Chain should be considered). 2) The analysis of the attacks does not show the impact of exploiting the vulnerability on the operation of the water system. • Question 2 part c 1) The mitigations are not related to MicroLogix 1100s PLC Your answer to question 1 is a reasonable attempt but it is not clear whether it is generic or whether you have given any consideration to the specific context of Cyprus. The ladder logic needs some attention – a few words of explanation would have helped. The answer to part b is also rather generic – we were looking for attacks that might run the pump dry or overfill the reservoir. The ICS-CERT alert for the specific vulnerability has some detailed mitigations – again, your answer is too generic.
FS518294	3	7+6+6+5=24 Total = 27/40	• Question 1 1) The direction of the arrows, which were drawn between the Electricity and transportation sectors, is reversed. 2) The figure does not show what the water sector provides to the transportation sector. • Question 2 Part a 1) The ladder logic is designed in a wrong way, as the pump will be set when the tank is full of water. 2) s1 and s2 are pressure sensors that shouldn't have the same value before and after the pump. Otherwise, the pump will not work. 3) There is no existing ladder logic for resetting the pump. • Question 2 part b 1) The analysis of the attack does not consider the IT domain (the two stages of the Cyber Kill Chain should be considered). Despite a few problems, as highlighted, you have made a good attempt at Q1. The ladder logic is incomplete and has a few problems. You describe the effect of the DDoS well; the attacker might also aim for the reservoir to overflow or the pump to run dry – this could be effected by updating the ladder logic through exploitation of the buffer overflow. Your answer about the mitigations is good.
1167163	4	7+6+8+3=24 Total = 28/40	• Question 1 1) The figure does not show the interdependencies between the water and transportation sectors. 2) The figure does not show what the water sector provides to the telecommunication sector. 3) The figure does not show what the transportation sector provides to the telecommunication sector. • Question 2 Part a

			1) Leakage detection in the tank using Sensor s6 is not considered in the ladder logic. 2) s1 and s2 are pressure sensors that shouldn't have the same value before and after the pump. Otherwise, the pump will not work. 3) Leakage and blockage detection in the pipe using Sensor s2, s3, and s4 are not considered in the ladder logic for resetting the pump. • Question 2 part b 1) The analysis of the attacks does not show the impact of exploiting the vulnerability on the operation of the water system. • Question 2 part c 1) The mitigations are not related to MicroLogix 1100s PLC You have done a lot of work for Q1 – this establishes the Cypriot context very well but seems to miss some potential dependencies. Are there 3rd and higher-order effects that should be considered? The attempt at the ladder logic is reasonable and it is helpful to have a narrative explanation. The answer on potential attacks is good and the penultimate paragraph identifies the potential impacts on the pump and reservoir. The mitigations are a bit generic – take a look at the ICS-CERT Alert.
1259070	4	6+8+9+3=26 Total = 30/40	• Question 1 1) The figure does not show the interdependencies between the water and transportation sectors. 2) The figure does not show what the water sector provides to the telecommunication sector. 3) The figure does not show what the transportation sector provides to the telecommunication sector. • Question 2 Part a 1) Leakage detection in the tank using Sensor s6 is not considered in the ladder logic. 2) Blockage detection in the pipe using Sensor s2 is not considered in the ladder logic. It is not clear to what extent the Cyprus context is considered in Q1, in addition to the points raised above. The narrative with the ladder logic is helpful and it is a reasonable attempt. The discussion of potential attacks is good. Try looking at the ICS-CERT alert for other potential mitigations but you have made some good suggestions.
922690	3	8+5+8+5=26 Total = 29/40	• Question 1 1) The interdependencies between the telecommunication, transportation, and water sectors are not clear. • Question 2 Part a 1) The ladder logic is designed in a wrong way, as the pump will be set even if the tank is full of water. 2) s1 and s2 are pressure sensors that shouldn't have the same value before and after the pump. Otherwise, the pump will not work.

			3) Each of these ladders is either incorrect or incomplete. Your answer to Q1 is clearly taking the Cypriot context into account. This is a good attempt. The ladder logic needs more attention as indicated above. The analysis of potential attacks is good. Well done for looking up the specific mitigations.
911033	1	5+5+5+3=18 Total = 19/40	• Question 1 1) Figure 1 does not show the interdependencies between the water and transportation sectors. 2) Figure 1 does not show what the transportation sector provides to the telecommunication sector. 3) Figure 2 does not show the effect of communication failure on other infrastructure sectors during the three different periods (i.e., a few minutes, a day and a week). • Question 2 Part a 1) Leakage detection in the tank using Sensor s6 is not considered in the ladder logic. 2) The ladder logic is designed in a wrong way, as the pump will be reset when there is water in the pipe. 3) s1 and s2 are pressure sensors that shouldn't have the same value before and after the pump. Otherwise, the pump will not work. • Question 2 part b 1. The analysis of the attacks does not show the impact of exploiting the vulnerability on the operation of the water system. • Question 2 part c 1. The mitigations are not related to MicroLogix 1100s PLC. Your answer to Question 1 is missing some detail and you have only considered 1st and 2nd order effects. It is not clear that you have considered the specifics of the Cyprus critical infrastructures. The narrative around the ladder logic is helpful but there are a few problems as indicated above. Your description of potential attacks is a start but, as indicated above, it would have been good to see more detail: for example, could the attacker run the pump dry, or empty/overfill the reservoir? You could have found some specific mitigations by looking at the ICS-CERT alert for this vulnerability.