Student ID	Grade	Comments
1084081	Q1 – 10 Q2a – 6 Q2b – 4 Q2c – 10 Q2d – 6 36/40	• Question 2 Part a 1) In designing the Ladder Logic, S2 was used to detect water leakage, but S2 should be used to detect water blockage, as S2 is a pressure sensor. 2) In case there is no water blockage, the pressure in the pipe is low. Consequently, S2 should be 0 to turn on the Pump. 3) In case S1=1 (on) {there is water in the borehole}, the Pump will not be turned on because of a flaw in designing the "reset" ladder logic. 4) S2, S3, S4 should be added to the design of "set" ladder logic. • Question 2 part c 1) The answer lacks the implementation of the kill chain steps on the example in question 2. But at least you have done some nice research on the CISA website. • Question 2 Part d 1) This is a good answer – you might also look at https://us-cert.cisa.gov/ics/advisories/ICSA-16-026-02 for mitigations.
918127	Q1 – 10 Q2a – 6 Q2b – 4 Q2c – 12 Q2d – 3 35/40	• Question 2 Part a 1) S2, S3, S4 should be added to to the design of "set" ladder logic. 2) In designing the Ladder Logic, S2 was used to detect water leakage, but S2 should be used to detect water blockage, as S2 is a pressure sensor. 3) In case there is water blockage, the pressure in the pipe is high. Consequently, S2 should be 1 (on) to turn off the Pump. • Question 2 Part d 1) The answer lacks the actual mitigation of the PLC vulnerability. Mainly based on Lockheed Martin notes. You could have looked at https://us-cert.cisa.gov/ics/advisories/ICSA-16-026-02 to see US Govt advice on mitigations.
1009533	Q1 – 10 Q2a – 6 Q2b – 2 Q2c – 8 Q2d – 3 29/40	• Question 2 Part a 1) S2, S3, S4 should be added to to the design of "set" ladder logic. 2) In designing the Ladder Logic, S2 was used to detect water leakage, but S2 should be used to detect water blockage, as S2 is a pressure sensor. 3) In case there is water blockage, the pressure in the pipe is high. Consequently, S2 should be 1 (on) to turn off the Pump. • Question 2 Part b 1) How can stealing the data from sensors disrupt the operation of the system? These data are not private data, so privacy is not an issue in the industrial control systems (ICSs). Your answer is too generic – you should be thinking about how the actual components of the system could be affected. • Question 2 Part c 1) The first stage of the kill chain is meant to be on the IT system rather than directly on the PLCs. • Question 2 Part d 1) The answer lacks the actual mitigation of the PLC vulnerability. See at https://us-cert.cisa.gov/ics/advisories/ICSA-16-026-02 to see US Govt advice on mitigations.