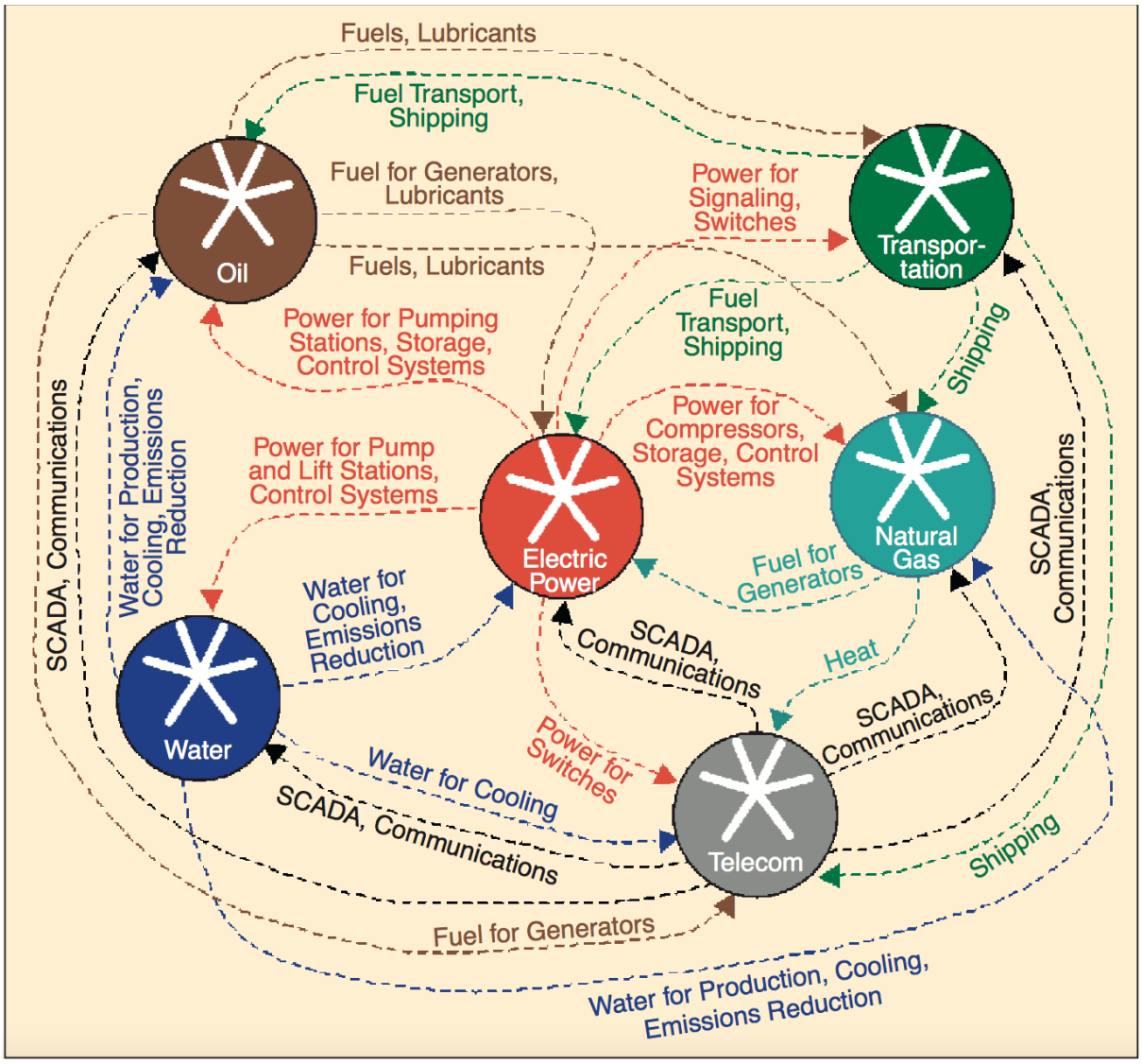
ECE803 Coursework

Tuesday, 15 November (Hand-in Wednesday 30 November)

Question 1

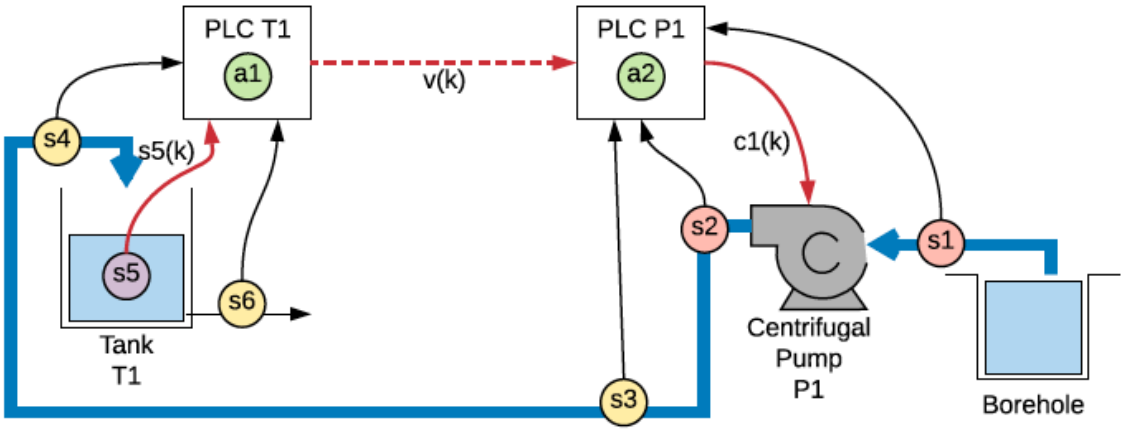
Seminal work by Rinaldi et al[1] studies dependencies between different infrastructures and they use graphs such as the following to identify such dependencies:



[1] *Identifying, Understanding and Analyzing Critical Infrastructure Dependencies*, Rinaldi, Peerenboom and Kelly, IEEE Control Systems Magazine, December 2001, doi: 10.1109/37.969131.

Considering the Electricity, Communications, Transportation and Water sectors in Cyprus, sketch a dependency diagram showing how these inter-relate. Construct a narrative, possibly using a ripple diagram or Rinaldi's consideration of nth-order effects, about how a failure in communications affects the other services – consider the first few minutes and then the effect of a blackout for a day and then a week. Note that your answer should be specific to the modern-day Cypriot context – this may be rather different from the examples in the notes.
(10=5+5)

Question 2
Consider the water distribution example from Part 2 of the notes:



Part a. PLC TI needs to detect low level in the tank and PLC P1 detects the presence of water at s1 and has the ability to start the pump. The sensors s1 and s2 are pressure sensors, s3, s4 and s6 are flow sensors and s5 is a level sensor. The parameter to s5 is a level reading and should be ignored for this exercise – instead treat s5 as a Boolean representing sufficient or insufficient water in the tank. Similarly, the parameter to c1 can be ignored and it can be treated as a Boolean that starts or stops the pump. Focussing mainly on s1, s5, the signal v (again ignoring the parameter) and the pump, sketch part of the ladder logic for the each of the PLCs.(10)

Part b. Suppose that the PLCs are MicroLogix 1100s with the vulnerability CVE-2016-0868 unpatched. Describe two ways in which an attacker might seek to disrupt the operation of this system. (10)

Part c. Suggest some mitigations to prevent these attacks. (5)