2009 Paper 7 Question 13

Security

Many critical industries, such as electricity, water, oil and gas, have plant controlled by complex digital systems. These "Supervisory Control and Data Acquisition" (SCADA) systems connect sensors, such as temperature and pressure gauges, with actuators, such as valves and switches, and control rooms. They were originally standalone systems and were thus designed without security mechanisms. However, over the last ten years, they have increasingly acquired Internet connectivity, and now there is serious concern about "cyberterrorism" in the form of online sabotage. As a result, the North American Electric Reliability Corporation (NERC) has ordered critical electricity utilities to protect their networks from 2009 or face substantial fines.

You have been hired by a utility that has several thousand devices on its central sites and several hundred at remote locations (the exact numbers are not known). These devices will disclose data to, or act on data from, anyone who communicates with them using the appropriate protocol.

(a) Discuss the advantages and disadvantages of the following protective strategies.

(i) Implementing fault-tolerant logic in the control system to identify and isolate faulty sensors. [4 marks]

(ii) Using a firewall to isolate the control system network from the corporate network and the Internet. [4 marks]

(iii) Authenticating traffic on the control system network by replacing sensors and actuators by, or supplementing them with, devices that can generate and verify message authentication codes. [4 marks]

(b) Your customer opts for strategy (ii) in respect of central sites and strategy (iii) for remote devices. Sketch an overall system design and discuss any residual risk. [8 marks]