2. (2 points) Company Safety Inc develops software for different kinds of power plants. They are specialized in the software that controls power plants' safety-critical operations. Describe how they could use security architecture for software development. Describe those items of security architecture that you consider especially important. Pick at least 4 items.

1. Company should apply defense in depth in case certain operation fails, machine stalls or some unknown event occurs. This could be handled by taking the machine in stand-by mode or completely shutting off the entire grid.
2. There should be a detailed description on how to take the machine from stand-by to fully operational and what's need to be fully checked off and what criteria needed to be fulfilled.
3. Since this is a power plant, we have to consider certain risk factor and there has to be clear concrete idea of
    a. What risks company are accepting
    b. What risks company are trying to avoid
    c. What risks company has fully mitigated
4. Every section of the power plant has to be under access rights and this will go in least privilege method.
5. Every actions should be able to traced back, in case of a hazard.
6. Use different standards set by compliance guidance and follow them through.

Please follow the principles of secure programming when implementing coding tasks.

You may use material section, especially Owasp and CERT coding standards. Please think about the following questions while preparing exercises.

- How can you make crypto safe random data? Why normal random function is not suitable?

Normal random function has a good mathematical probabilistic property, which makes it bad for crypto.

- What does race condition mean? How reading and writing a file may cause race condition vulnerability?

Read before write, or write before read. Race condition means trying to access the same file or resources at the same time.

- What possible vulnerabilities are related to command line parameters?

- What is the difference between validation and sanitation?

Validation checks inputs against certain criteria, it changes depending on the system or requirements. Sanitation checks if the given input is safe for program, its same for almost all cases. Certain words or phrases or characters cannot be used in certain system but it does not check if the input is actually what the system wants. For example: sanitation will check if the given input is not an SQL Injection but it will not check if it’s a string or a number or an email and what’s actually required, validation will figure that out.

- Can you trust in exercise 3, that sanitation works correctly in all situations? Why?

No, the algorithm I use is not cryptographically secure pseudo random number.