

Question 1: Security Property Writing For each security policy below, identify:

- the **asset** being protected;
- the **forbidden behavior**;
- a possible **security property** written using simple pseudocode or mathematical notation; and
- a possible **counterexample**: a sequence of events or system state that would demonstrate that the property has been violated.

Your property does **not** need to use formal verification syntax. The goal is to make the security policy more precise.

1.1. Policy A: User code should not modify a privileged configuration register.

1. Asset:

2. Forbidden behavior:

3. Security property:

4. Possible counterexample:

1.2. Policy B: Once a security lock is enabled, the protected register should not change.

1. Asset:

2. Forbidden behavior:

3. Security property:

4. Possible counterexample:

1.3. **Policy C:** A debug interface should not write protected state until authentication succeeds.

1. Asset:

2. Forbidden behavior:

3. Security property:

4. Possible counterexample: