

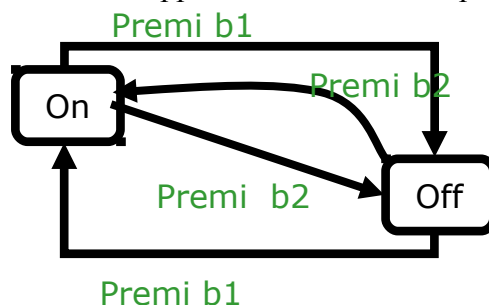
Linguaggi di Programmazione per la Sicurezza

Progettazione di Software Sicuro

Progettazione di Software (prima parte)

Esame del 28 Gennaio 2014 – (Parte Scritta)

1. Descrivere tre possibili attacchi. [pt. 3]
2. Descrivere i principi su cui si basa il *design by contract* e gli elementi che costituiscono un contratto [pt. 3]
3. Dato la seguente FSM, dare la sua rappresentazione in state pattern [pt. 3]



4. Modellare con una macchina UML a stati paralleli il comportamento del seguente sistema di controllo di una porta della metropolitana. Il sistema è costituito da un controller e da tre sensori: il sensore *arrived* che rileva l'arresto della metro alla stazione, il sensore *status* che segnala l'avvenuta apertura/chiusura delle porte ed il sensore *pass_person* che rileva il passaggio di una persona che vuole entrare nella metro quando le porte si stanno chiudendo. Su segnalazione del sensore *arrived*, il controller invia il comando di apertura alle porte della metro e poi aspetta il segnale di avvenuta apertura. Passato un minuto dall'apertura completa delle porte, il controller aziona la chiusura delle porte ed attende il segnale di avvenuta chiusura. Se il sensore *pass_person* rileva il passaggio improvviso di persona, le porte vengono immediatamente riaperte. Il controller provvederà nuovamente alla chiusura delle porte. Periodicamente, ogni mese, il sistema è soggetto ad un fase di manutenzione della durata di una settimana. Durante la manutenzione viene controllato il corretto funzionamento della porta e dei sensori. [pt. 5]
5. Dare la definizione di test set affidabile, valido ed ideali. Dato il seguente programma:

```
program raddoppia(input, output)
  var x, y : integer;
  begin
    read(x)
    y:= x*x;
    write(y)
  end
```

classificare i seguenti test set in affidabili, validi ed ideali.
T1={{0}, {0,2}}; T2={{0,1},{2,3}}; T3={t | t > 3}; T4={ t | t numero dispari} [pt.3]
6. Determinare i casi di test per l'MCDC della seguente decisione $((x > 1) \ \& \ (y \neq 0)) \parallel (z < 0)$ [pt. 3]