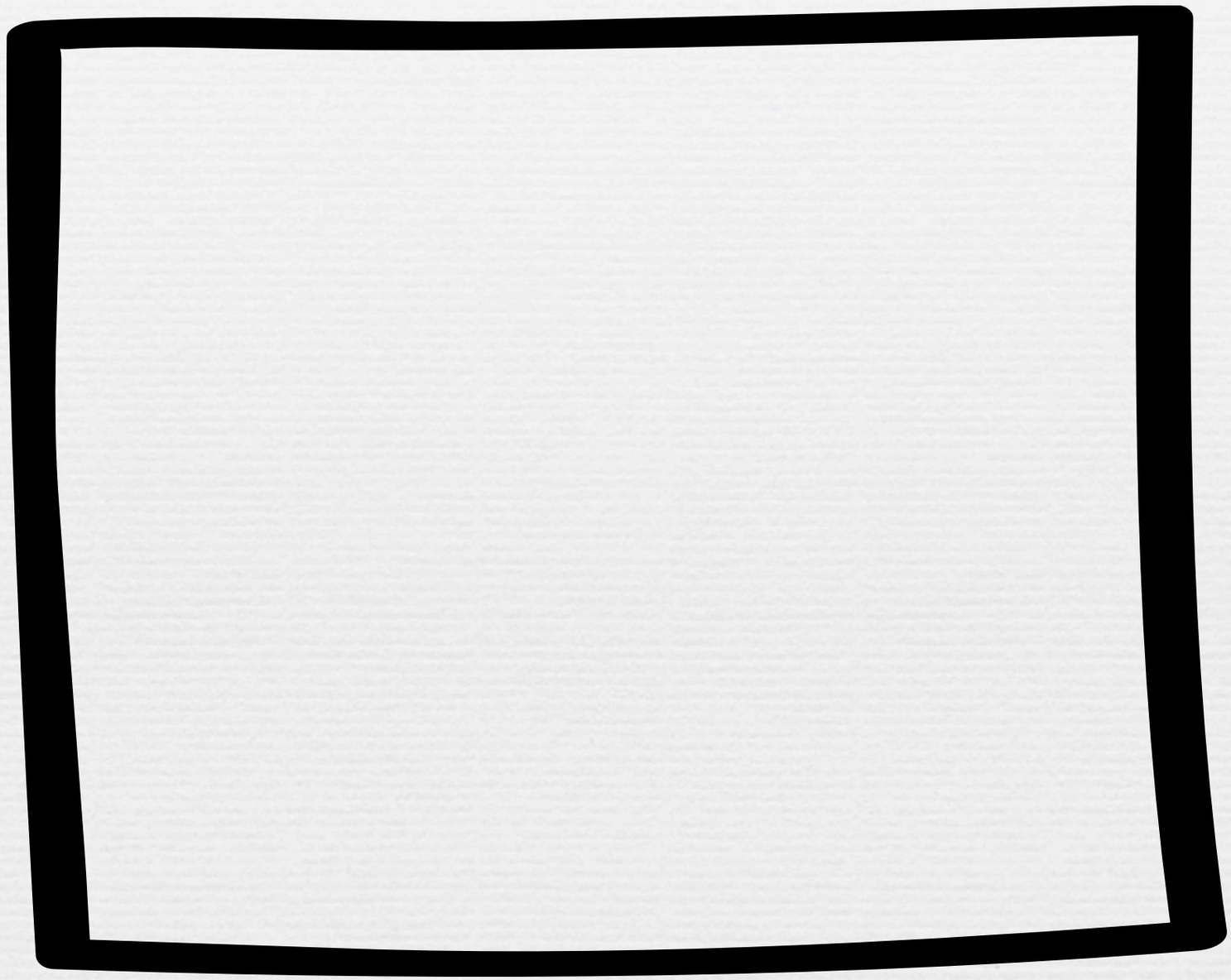
introduzione al fuzz testing

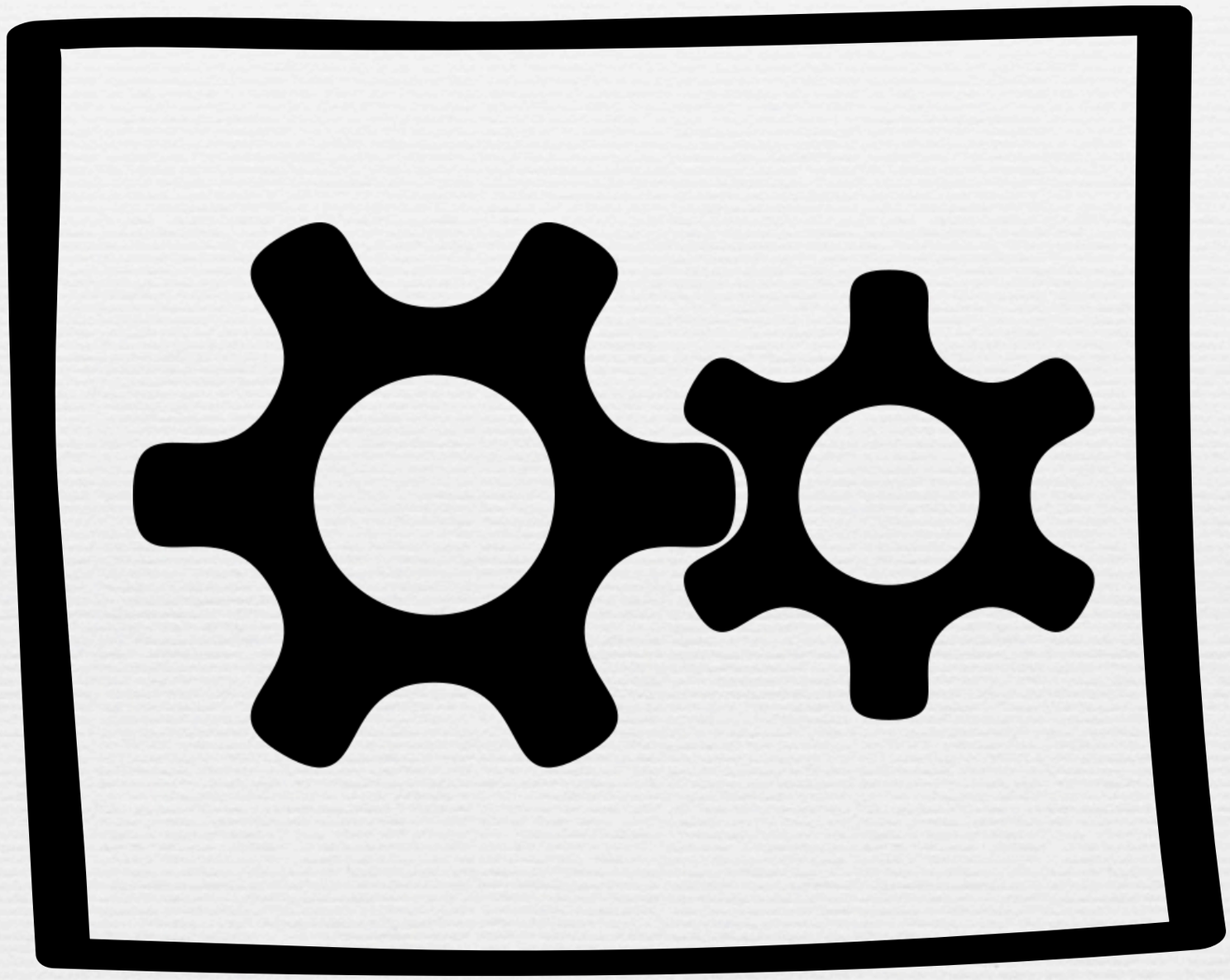
@federicocaboni

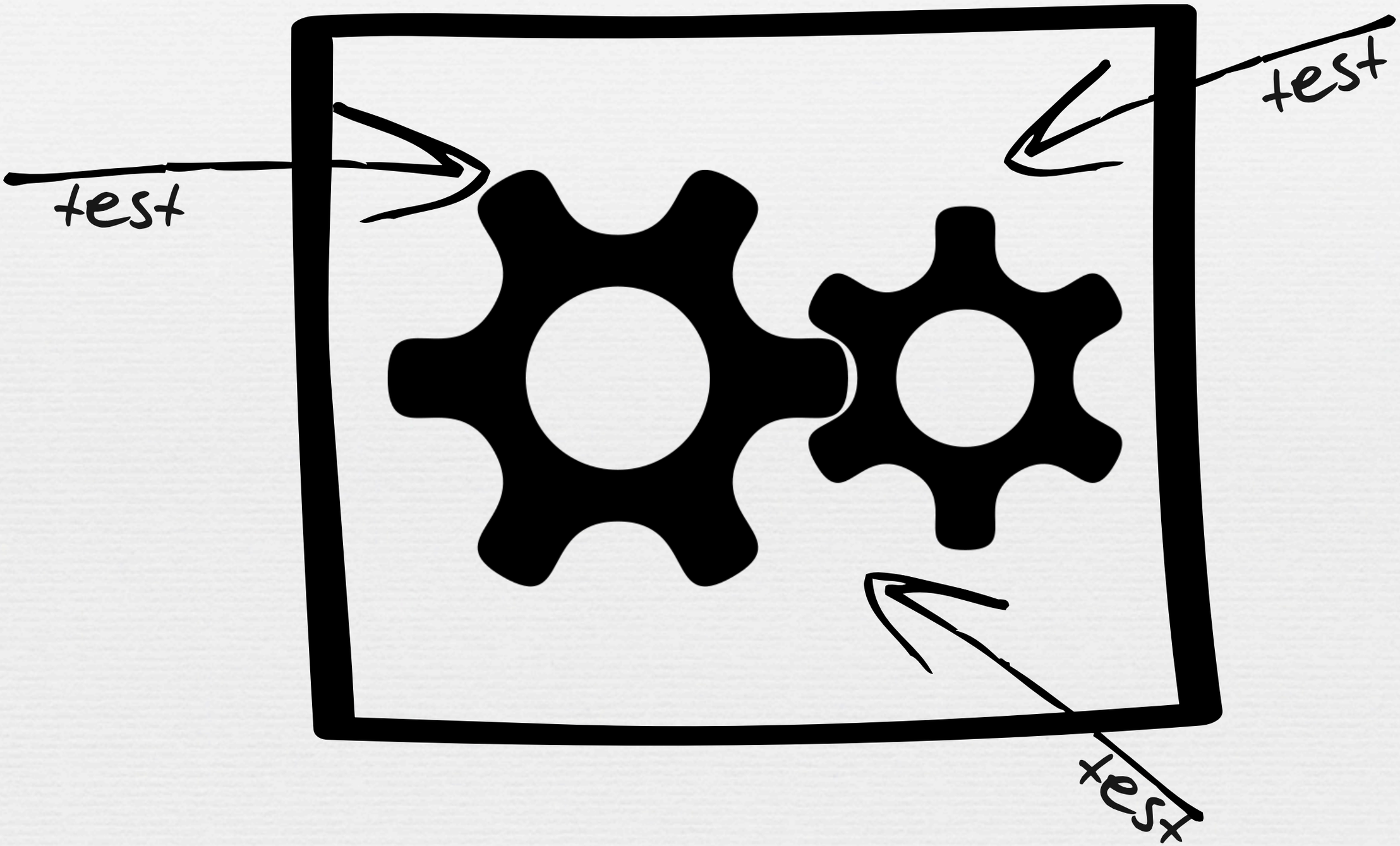
http://www.linkedin.com/in/fcaboni

TESTING

IL SOFTWARE FA SCHIFO






test
test
test

INFORMALE

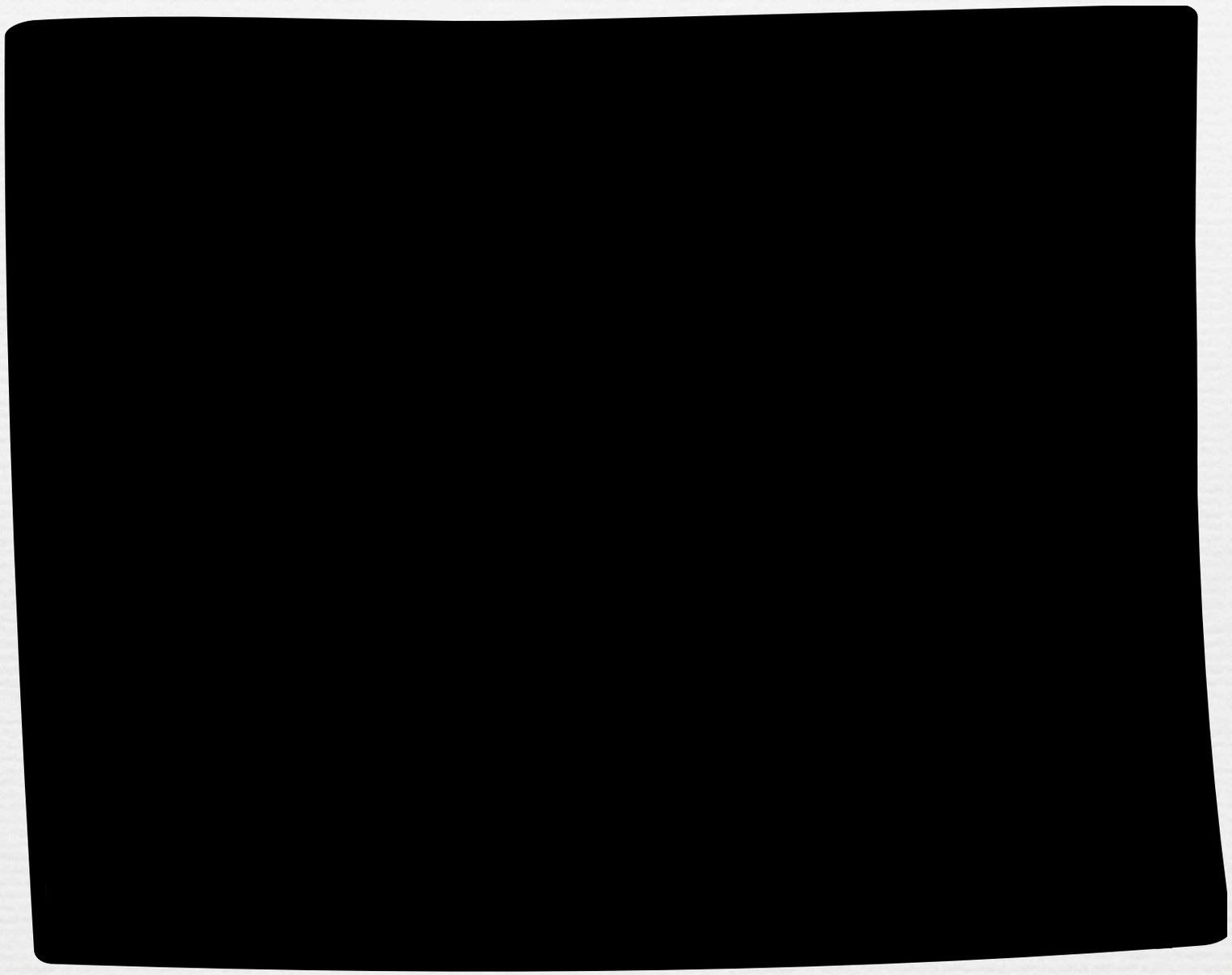
```
print(“x qui vale”,x)
```

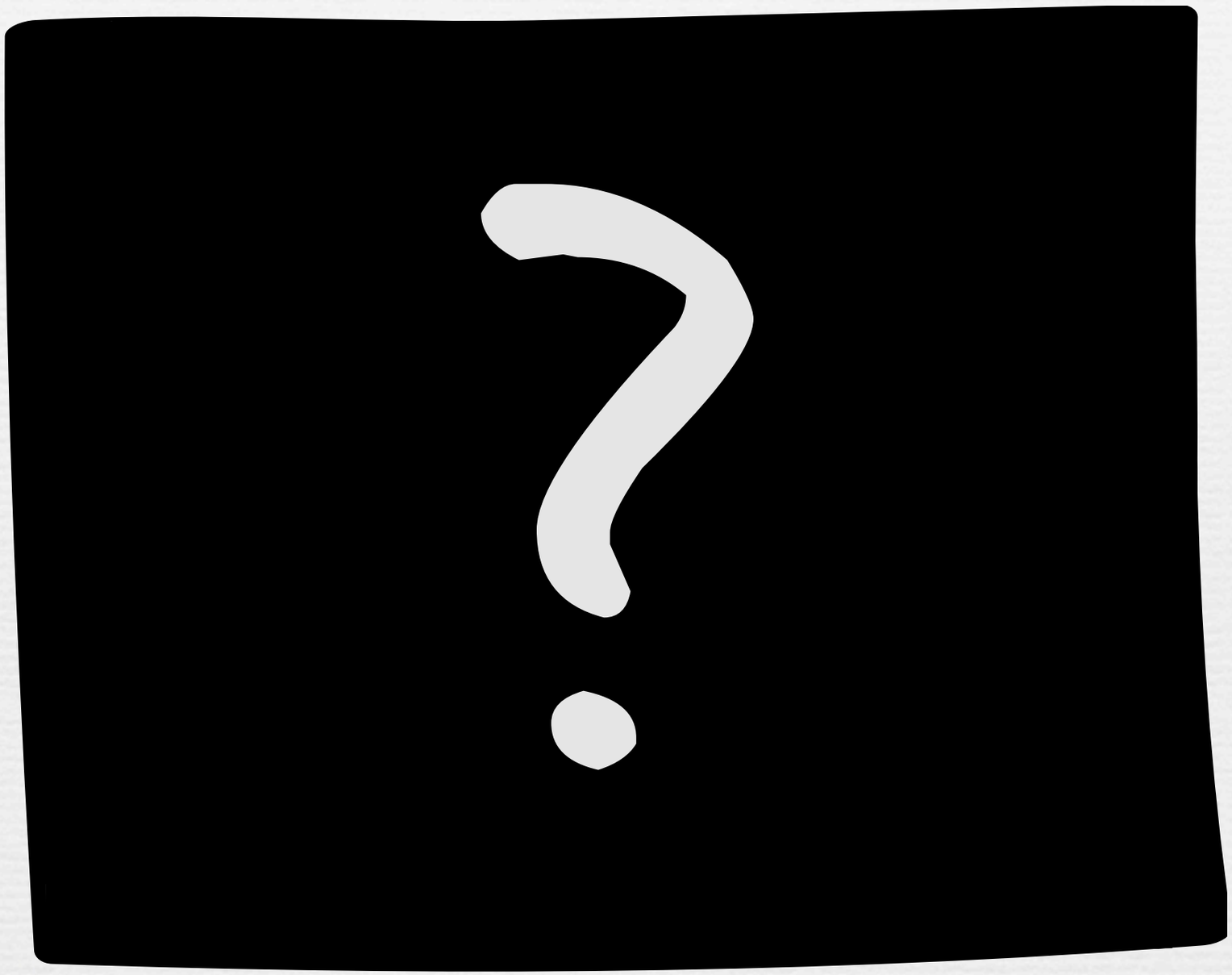
UNIT TEST

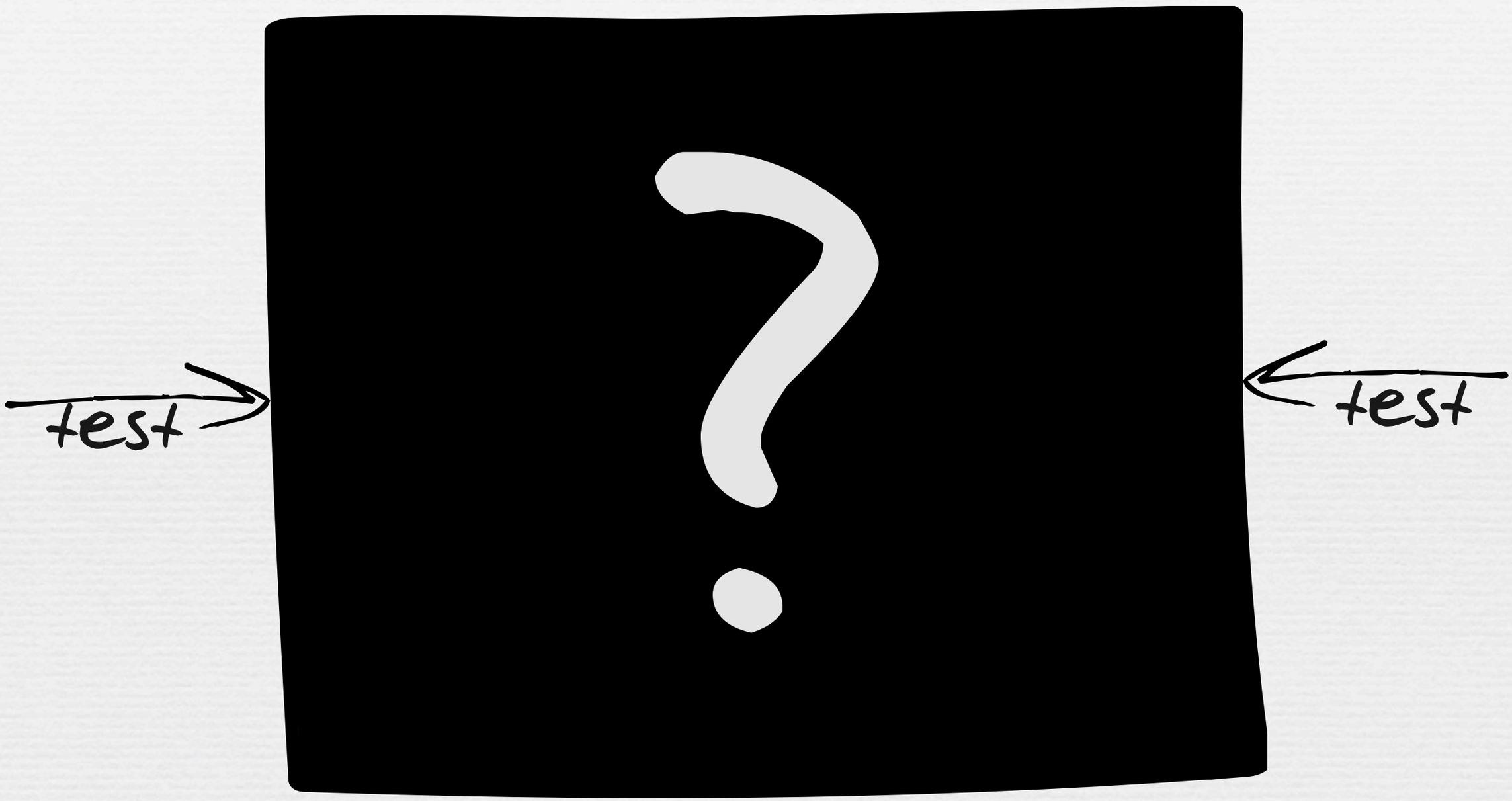
```
public class TestAdder {

    public void testSumPositiveNumbersOneAndOne() {
        Adder adder = new AdderImpl();
        assert(adder.add(1, 1) == 2);
    }

    public void testSumPositiveNumbersOneAndTwo() {
        Adder adder = new AdderImpl();
        assert(adder.add(1, 2) == 3);
    }
}
```






test
test

Open Test Manager - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:5050/testlist

Go

Open Test Manager

Main Page | Test Cases | Testers | Help | Logout

Test Cases

Test Case	Status	Area	Level	Assigned To
#1: Login	Pass	Data	1	Fredrik Fornwall
#2: Just Testing	Pass	Design	2	Goran Soderman
#3: Adding a new user to the testers list	Fail	Design	2	Faina Barknell
#4: Print a project summary	Fail	Design	2	Faina Barknell
#5: Export to PDF	Not Tested	Design	2	Faina Barknell
#6: Sample TestCase 0	Not Tested	Design	2	Faina Barknell
#7: Sample TestCase 1	Not Tested	Design	2	Faina Barknell
#8: Sample TestCase 2	Not Tested	Design	2	Faina Barknell
#9: Sample TestCase 3	Not Tested	Design	2	Faina Barknell
#10: Sample TestCase 4	Not Tested	Design	2	Faina Barknell

Done

TECNICHE DETERMINISTICHE

input vuoto (file, 0, ecc)

input malformato

fuori range

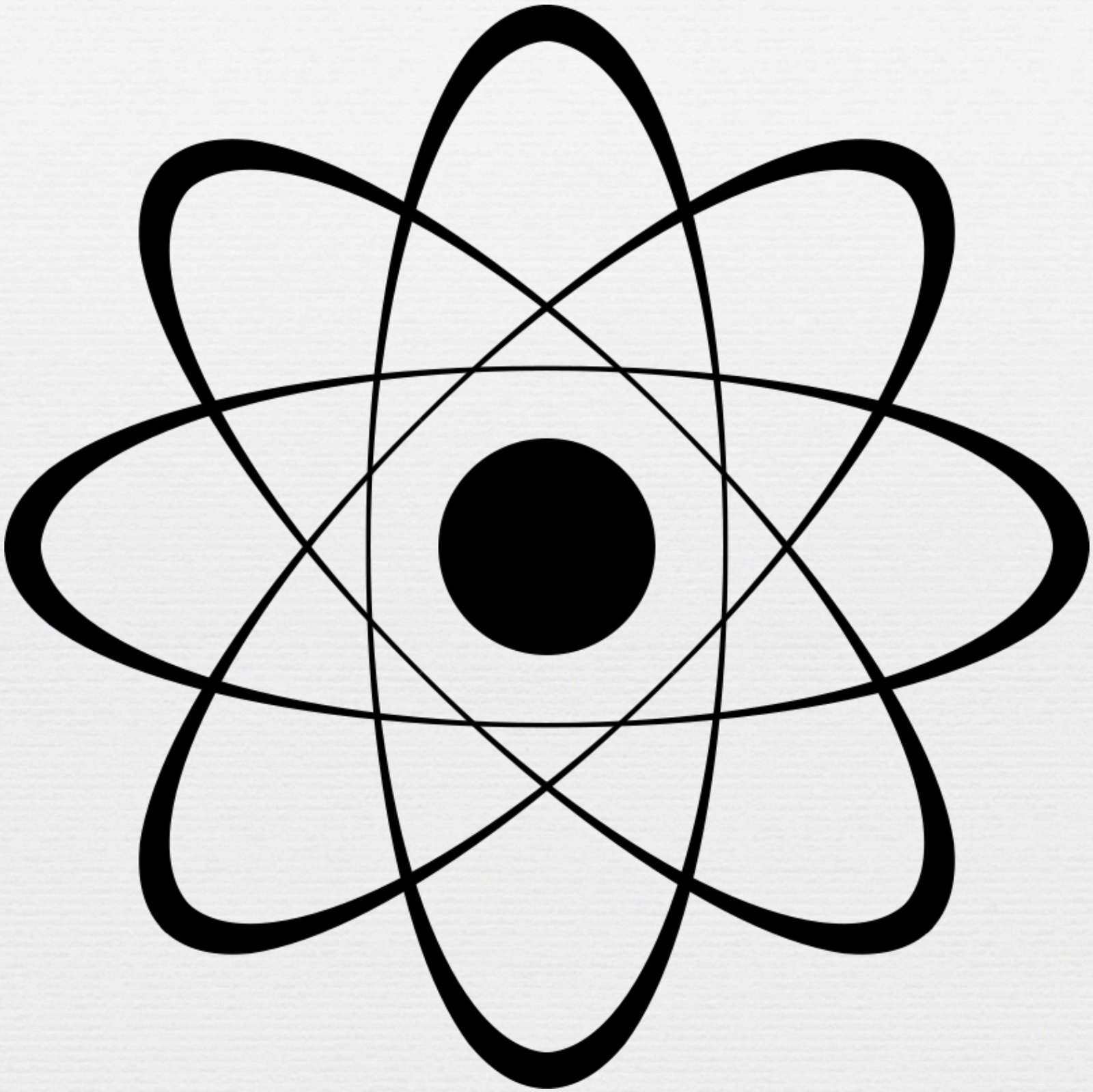
tipo sbagliato

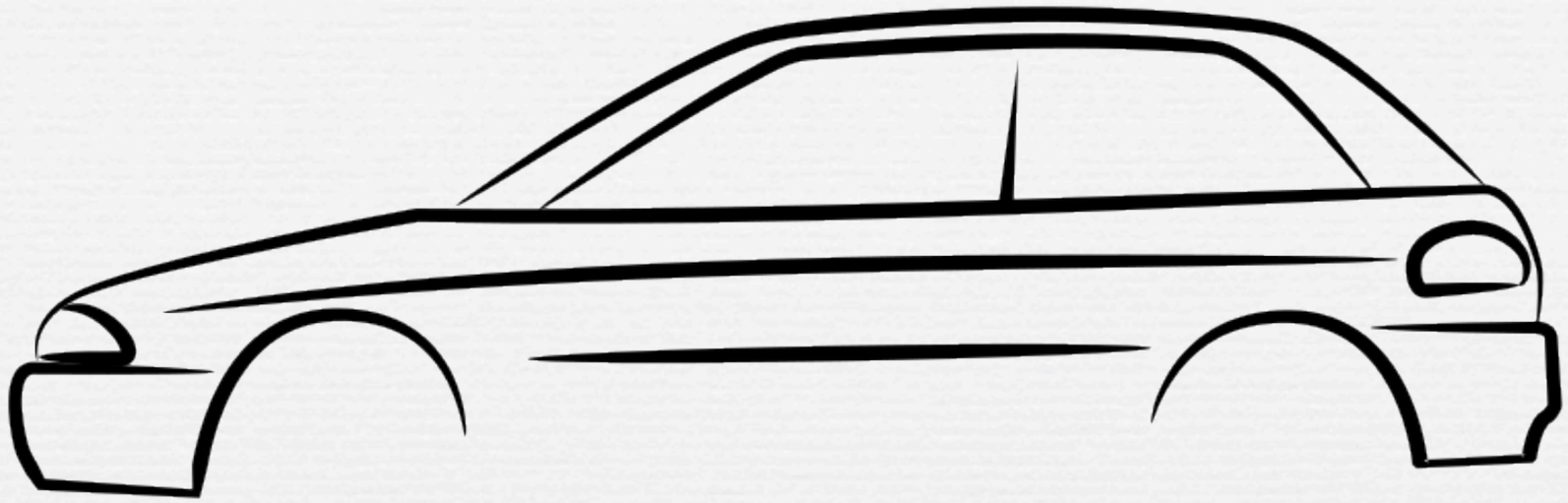
bug che si sono già verificati

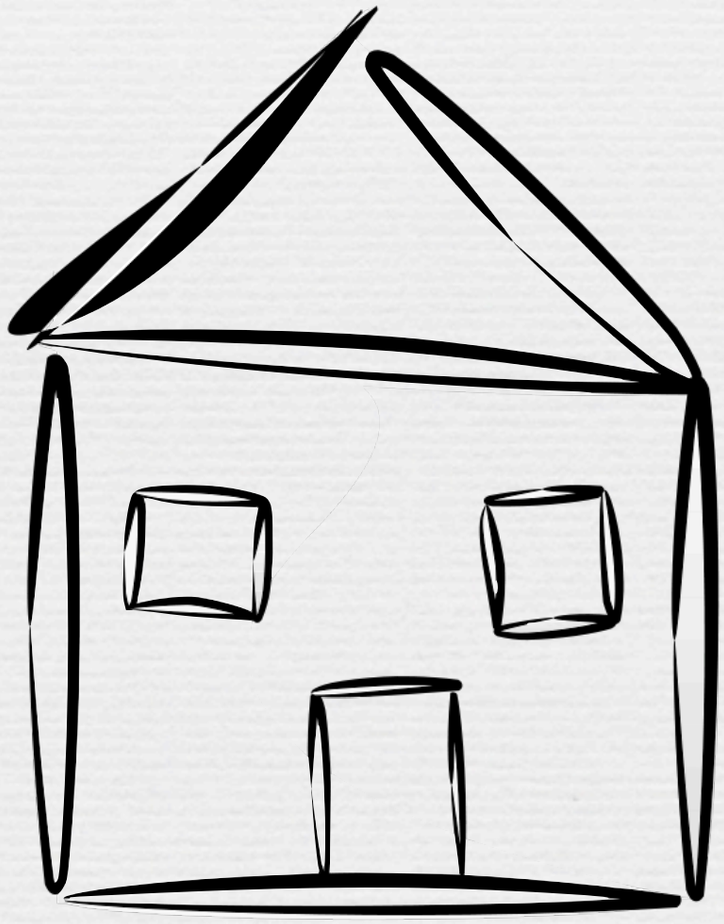
errori comuni (indici degli array, ecc...)

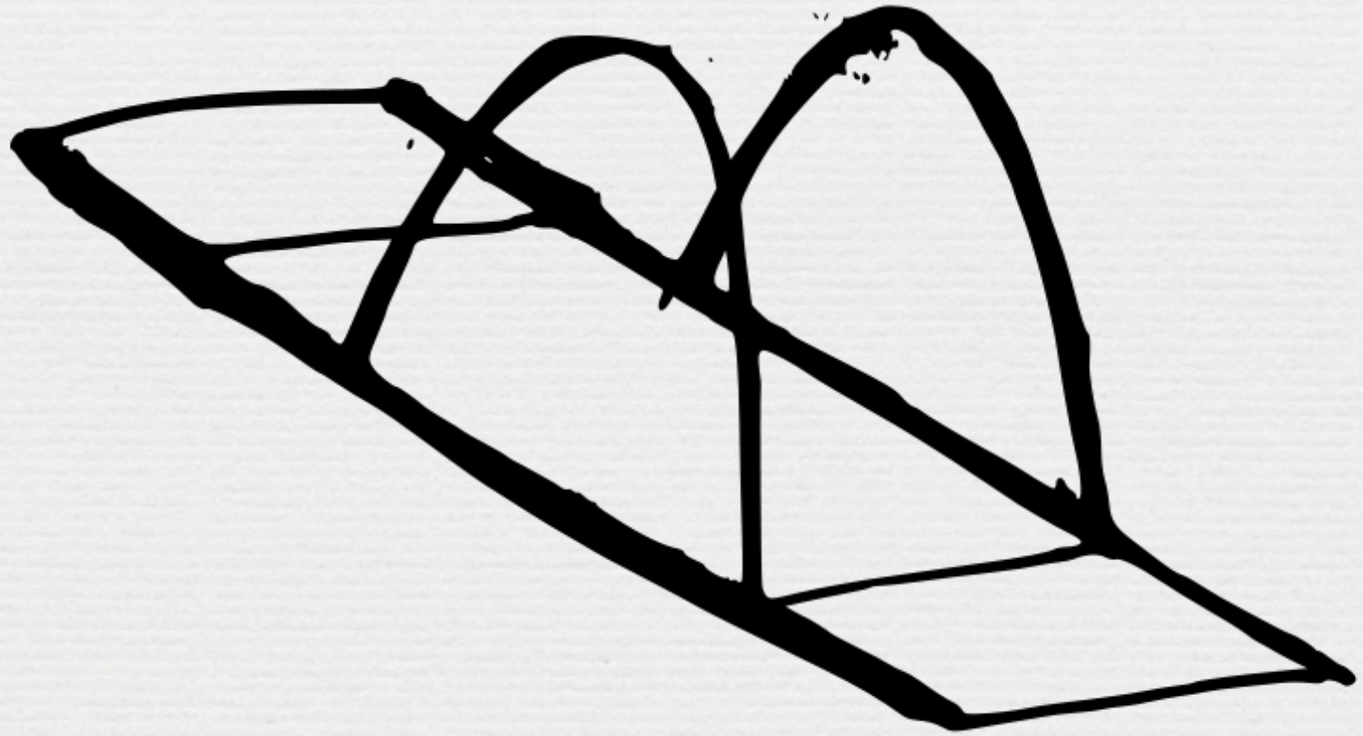
comportamenti previsti dalle specifiche

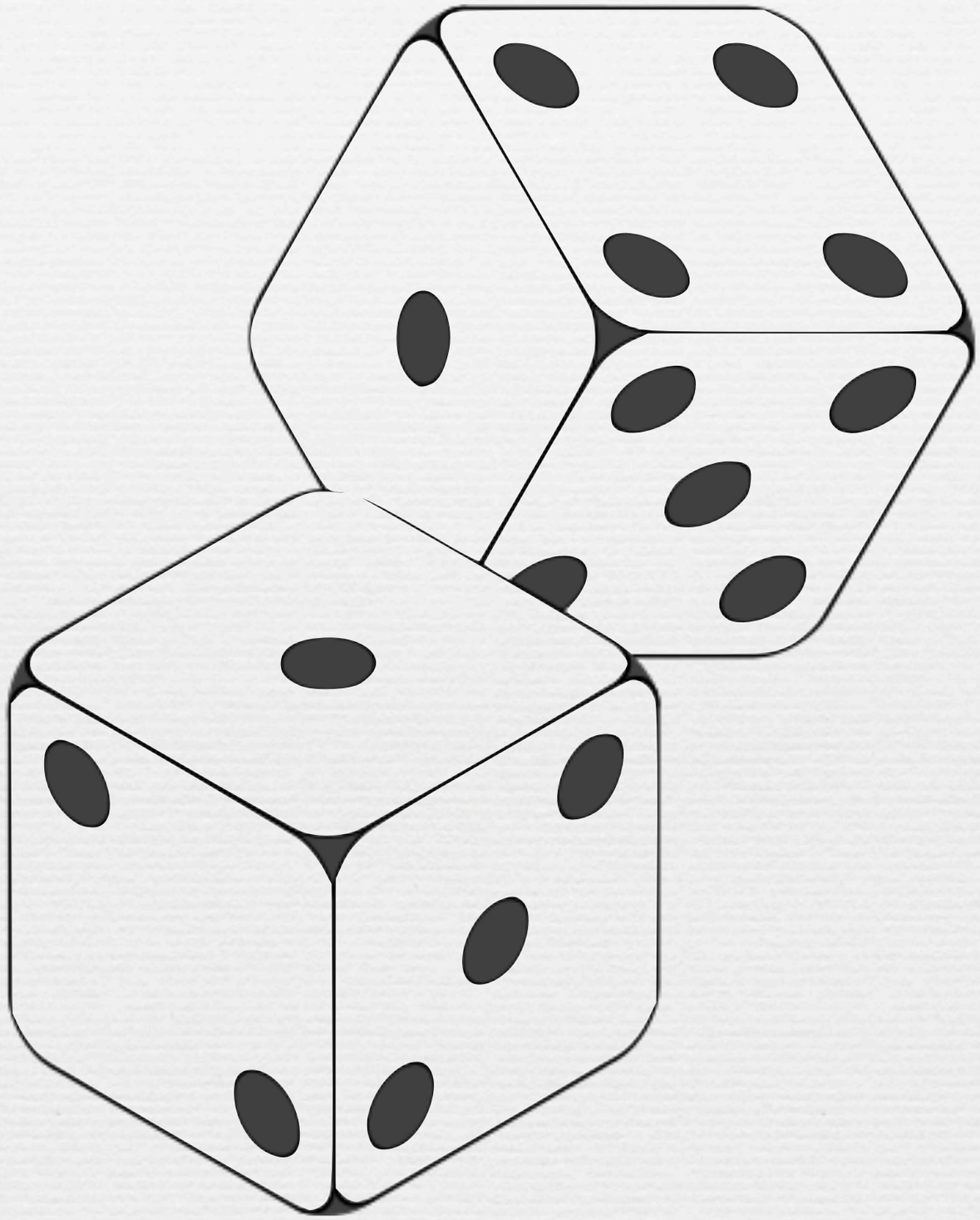
And now, for something completely different...











FUZZ TESTING

FUZZING

corruzione random di dati

ha trovato (dozzine di) bug in mplayer, vlc, libpng, Quicktime, OS X, X, xpdf, VMWare, Adobe Reader,...

nasce da un progetto didattico nel 1988, in un corso di Barton Miller, University of Wisconsin.

usato da Microsoft per irrobustire sensibilmente il supporto ai formati di file in Office 2007

il 33% circa dei comandi UNIX provati aveva dei bug!

An Empirical Study of the Reliability of UNIX Utilities, CACM 33,12. 1990. B. Miller, L. Fredriksen

APPLICA L'APPROCCIO PROBABILISTICO AL TESTING DEL SOFTWARE

GENERAZIONE

VS

MUTAZIONE

000000000

00010000

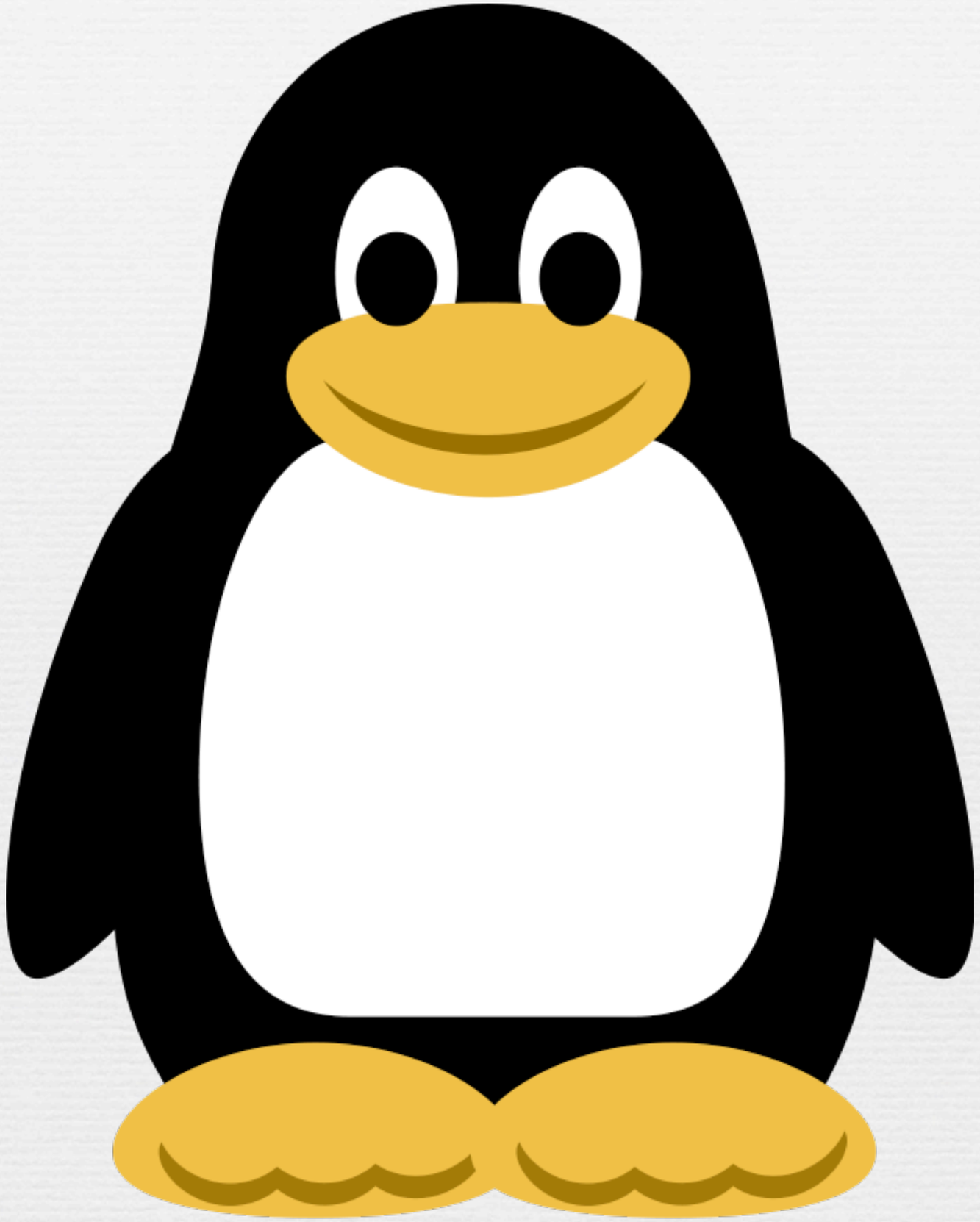

ZZUF

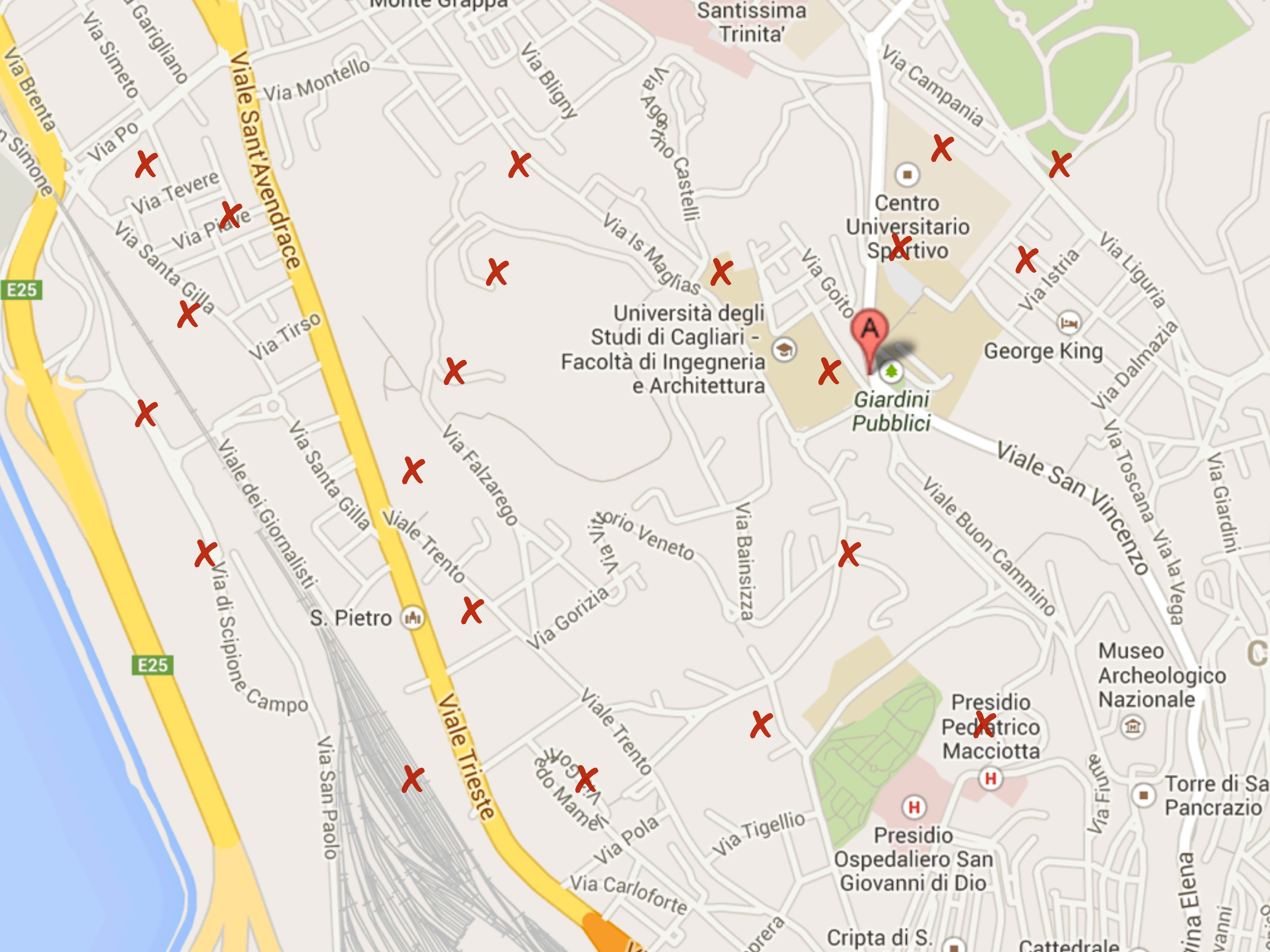
0x20 (32) SPAZIO

0x22 (34) “

00100010

UN ESEMPIO




Monte Grappa
Santissima Trinita'
Via Brenta
Via Simeto
Via Garigliano
Viale Sant'Avendrace
Via Montello
Via Bligny
Via Agostino Castelli
Via Campania
Via Po
Via Tevere
Via Piave
Via Santa Gilla
Via Tirso
Via Is Maglias
Centro Universitario Sportivo
Via Goito
Via Istria
Via Liguria
Università degli Studi di Cagliari - Facoltà di Ingegneria e Architettura
A
George King
Via Dalmazia
Giardini Pubblici
Viale San Vincenzo
Via Toscana
Via la Vega
Via Giardini
E25
Viale dei Giornalisti
Via Santa Gilla
Via Falzarego
Viale Trento
Vittorio Veneto
Via Bainsizza
Viale Buon Cammino
Via di Scipione Campo
S. Pietro
Via Gorizia
Museo Archeologico Nazionale
Viale Trento
Presidio Pediatrico Macciotta
Via San Paolo
Viale Trieste
Via Fiume
Torre di San Pancrazio
Via Pola
Via Tigellio
Presidio Ospedaliero San Giovanni di Dio
Via Carloforte
Cripta di S.
Cattedrale
Via Elena

PMN
(PENGUIN MONITORING NETWORK)

i rilevatori di pinguini sono installati in giro per Cagliari

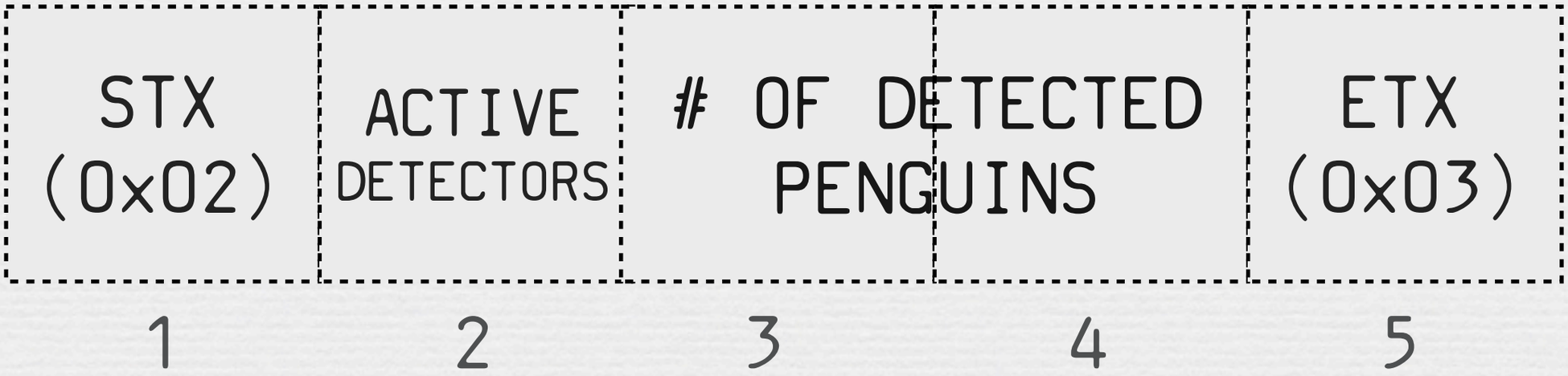
ognuno di loro invia un ping a una stazione di controllo centrale ogni volta che individua un pinguino

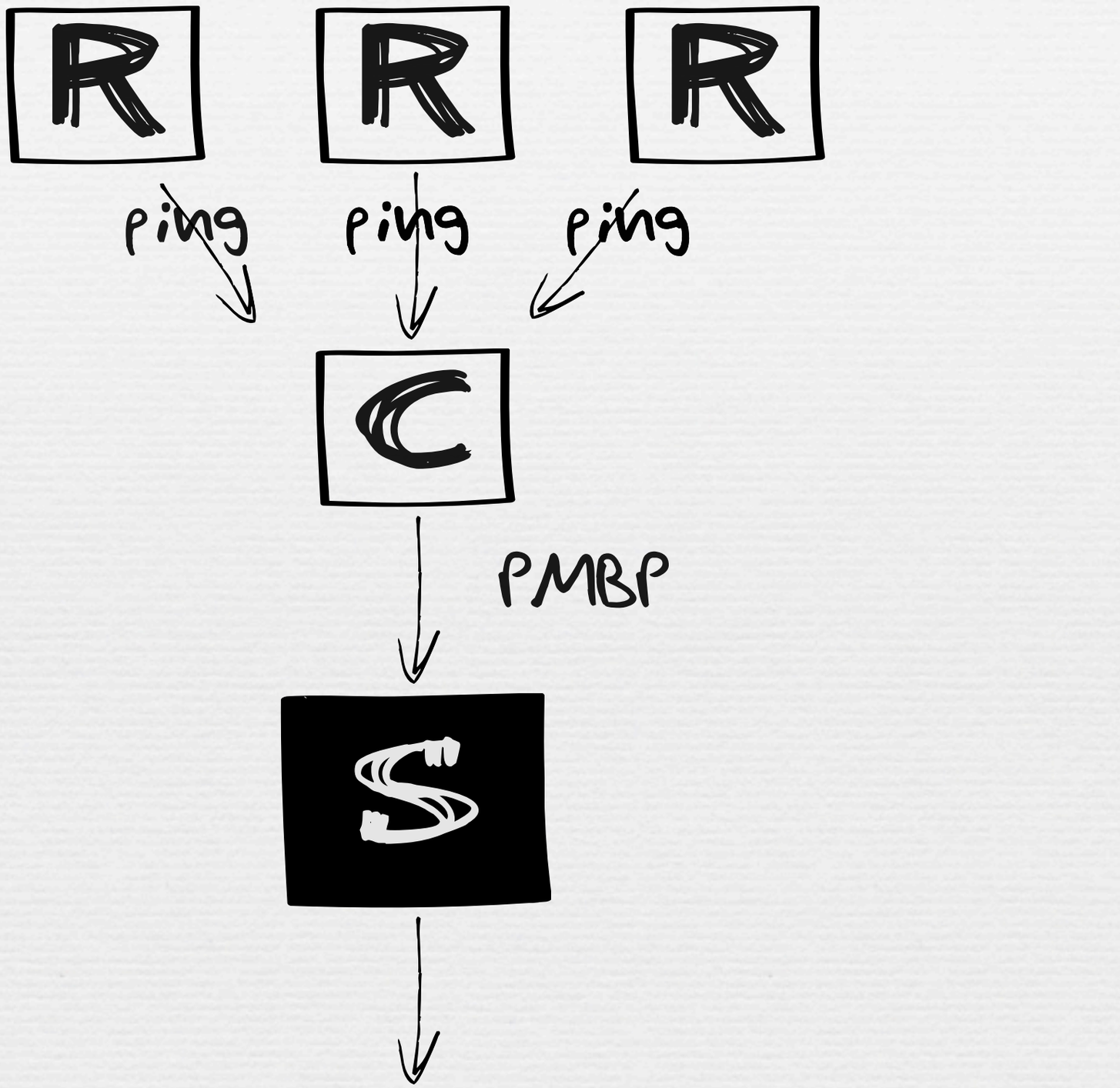
la stazione di controllo centrale invia giornalmente al nostro server un messaggio binario che contiene il numero totale di pinguini individuati

il compito del programma è fare il parsing del messaggio binario e ritornare il parametro APPD (Average Penguins Per Detector)

PMBP

(PENGUIN MONITORING BINARY PROTOCOL)




R
R
R
ping
ping
ping
C
PMBP
S
APPD (Average Penguins Per Detector)

ZZUF

intercetta le syscall

riproducibile

output dipendente <u>solo</u> dai dati

escusione di file/caratteri/offset

FUZZ TESTING

ottimo rapporto costi/benefici
trova bug diversi
approccio probabilistico
black box testing
ottimo per sicurezza, formati di file

@federicocaboni

http://www.linkedin.com/in/fcaboni

GRAZIE!!

federico.caboni@me.com