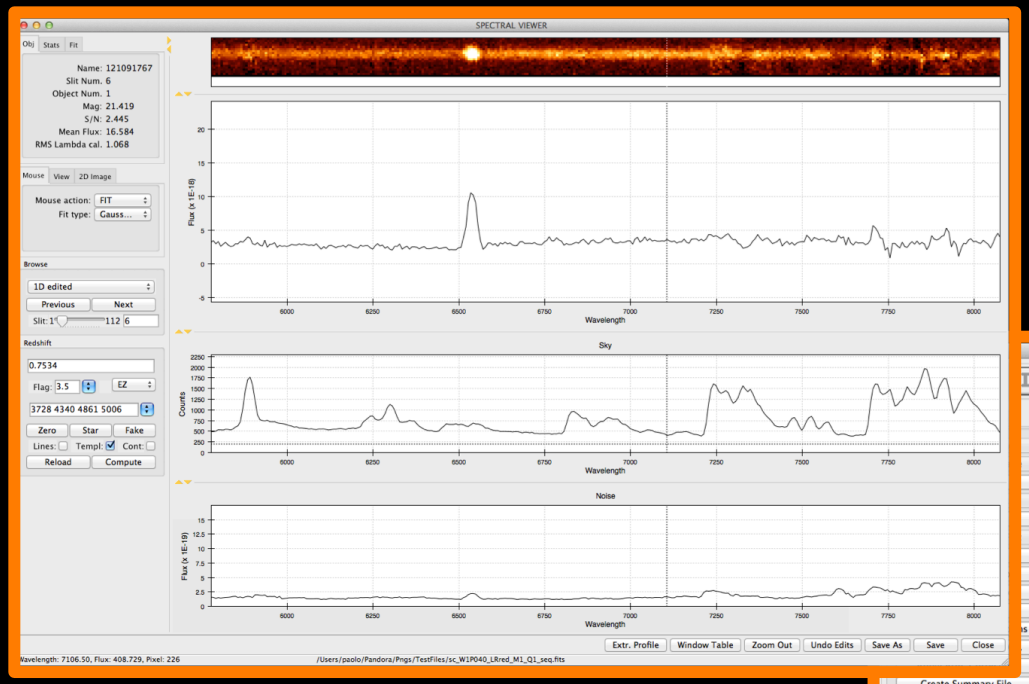
bugbusters

disinfestatori di software

Paolo Franzetti

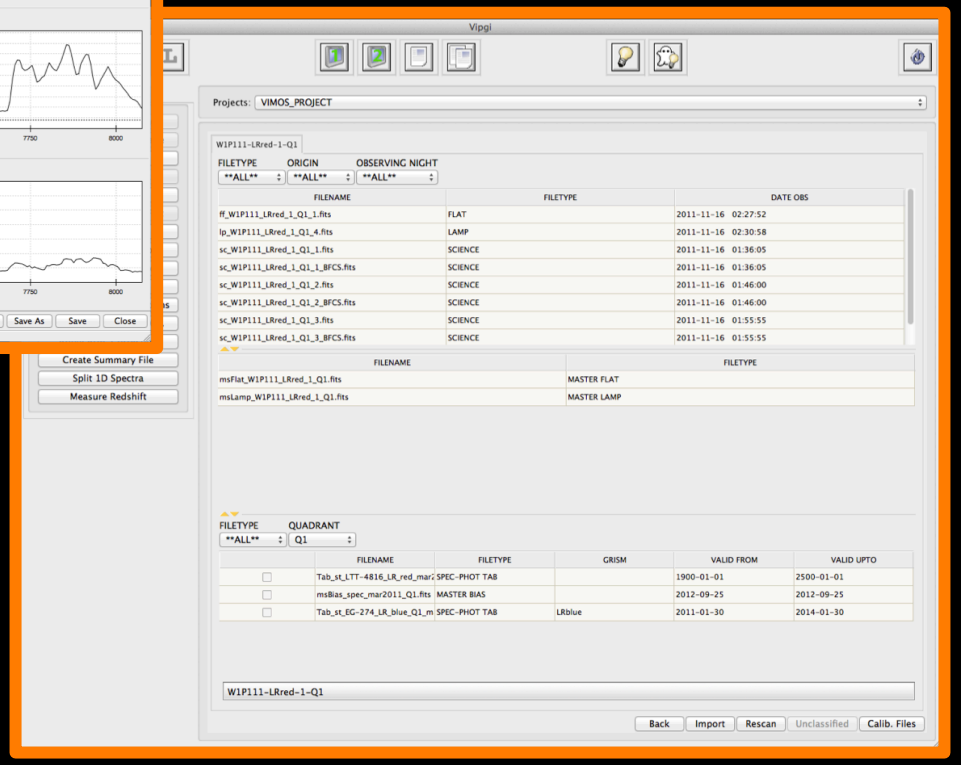
Astrosiesta – 9/4/2015

una doverosa premessa



pandora.ez

pandora.vipgi



il nemico

cos’è un *bug*

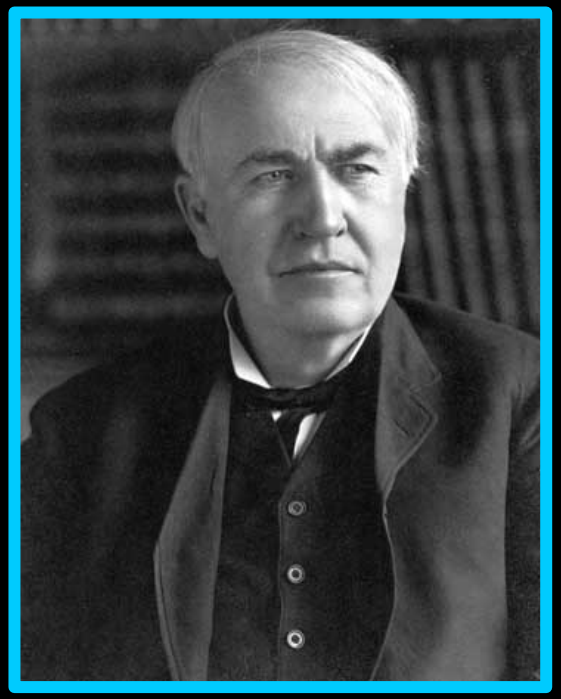
wikipedia dixit il nemico

a software bug is an error, flaw, failure,
or fault in a computer program or system
that causes it to produce an incorrect
or unexpected result,
or to behave in unintended ways

etimologia il nemico

It has been just so in all of my inventions. The first step is an intuition, and comes with a burst, then difficulties arise - this thing gives out and then that bugs - as such little faults and difficulties are called - show themselves and months of intense watching, study and labor are requisite before commercial success or failure is certainly reached

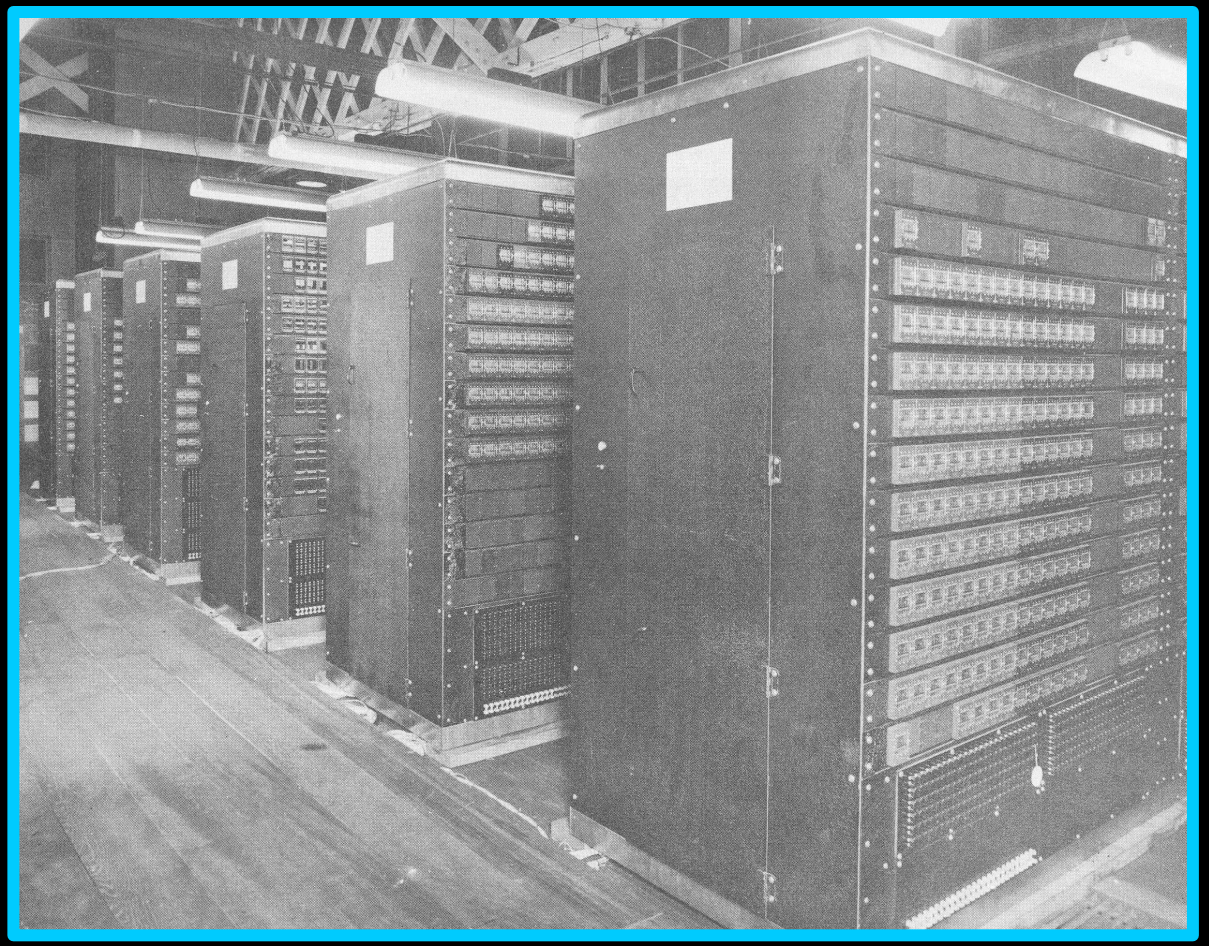
Thomas Edison, 1878



etimologia il nemico

Grace Murray Hopper, 1947

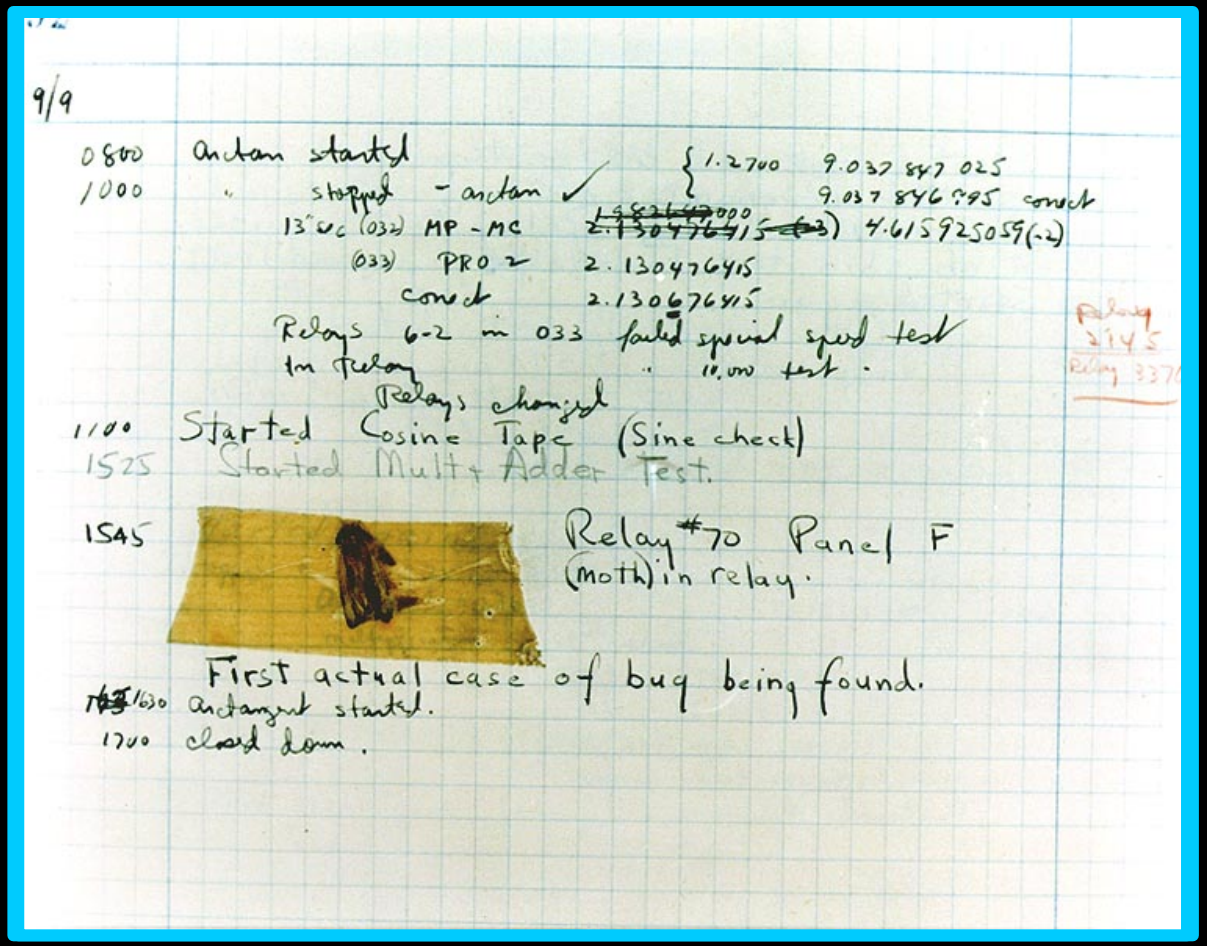
Harvard Mark I
(16 x 2.4 x 0.61 m, 4500 kg)



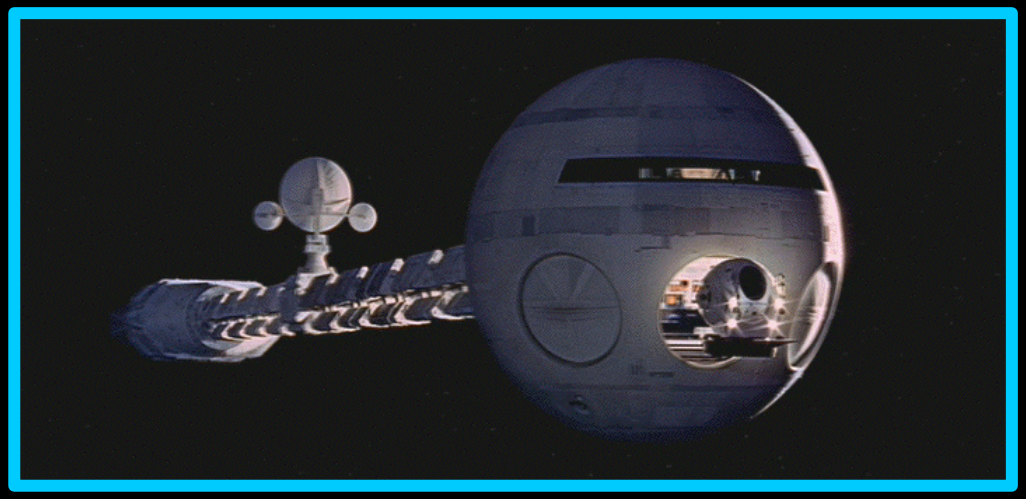
etimologia il nemico

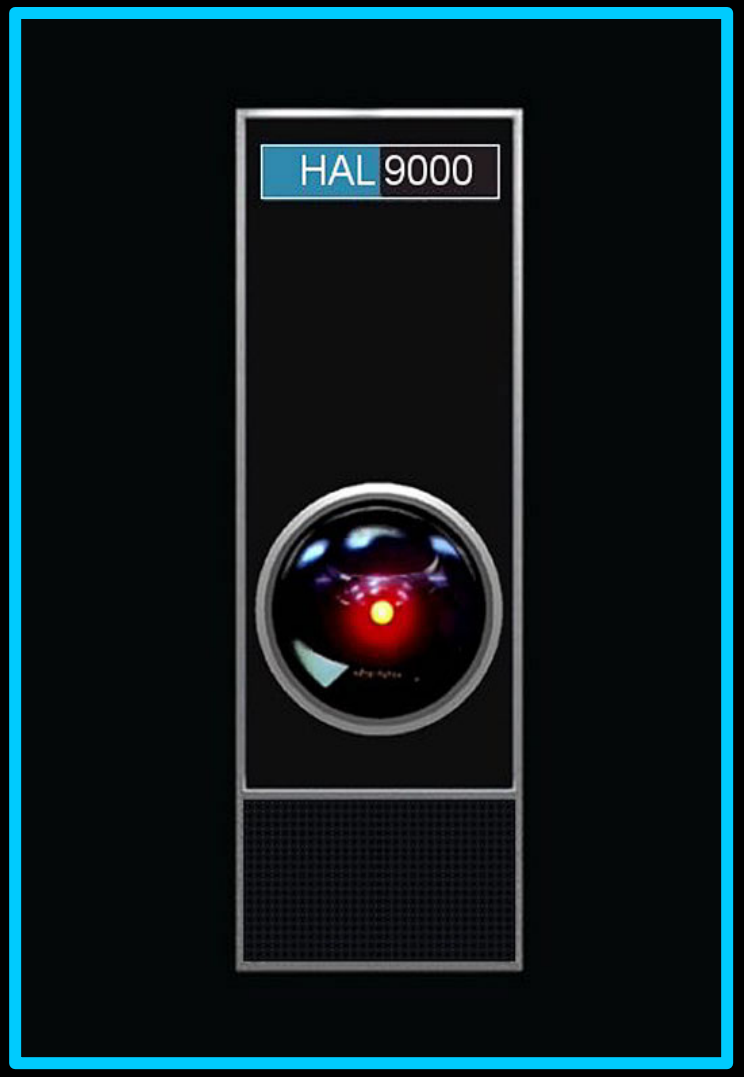
Grace Murray Hopper, 1947

Harvard Mark I
(16 x 2.4 x 0.61 m, 4500 kg)



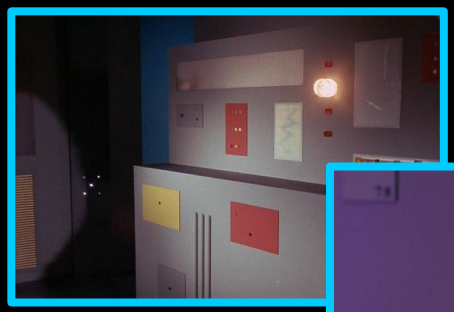
sci-fi il nemico

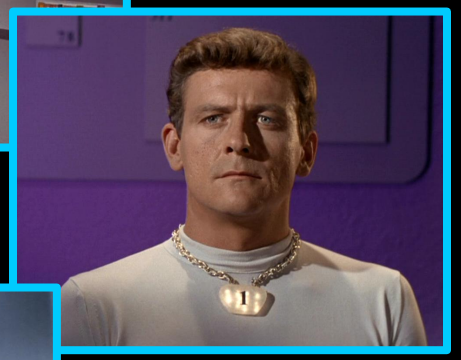


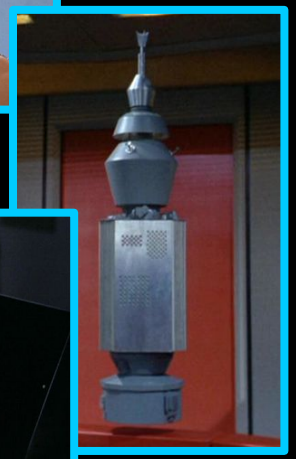


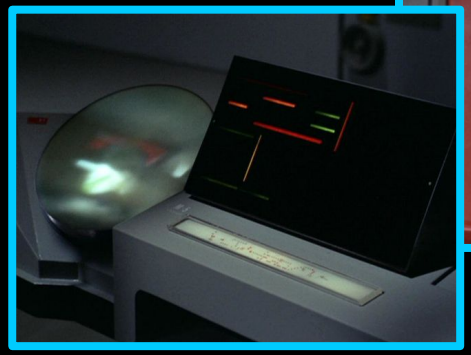
- Open the pod bay doors, HAL.
- I'm sorry, Dave. I'm afraid I can't do that.

sci-fi il nemico









“ You say you are lying, but if everything you say is a lie then you are telling the truth, but you cannot tell the truth because everything you say is a lie, but... you lie, you tell the truth, but you cannot for you... Illogical! Illogical! Please explain! ”

l’esercito

in quanti modi si può sbagliare

i tipi l'esercito

Arithmetic bugs
- Division by zero.
- Arithmetic overflow or underflow.
- Loss of arithmetic precision due to rounding or numerically unstable algorithms.

Logic bugs
- Infinite loops and infinite recursion.
- Off-by-one error, counting one too many or too few when looping.

Syntax bugs
- Use of the wrong operator, such as performing assignment instead of equality test.

Resource bugs
- Null pointer dereference.
- Using an uninitialized variable.
- Using an otherwise valid instruction on the wrong data type.
- Access violations.
- Resource leaks, where a finite system resource become exhausted by repeated allocation without release.
- Buffer overflow, in which a program tries to store data past the end of allocated storage.
- Excessive recursion which — though logically valid — causes stack overflow.
- Use-after-free error, where a pointer is used after the system has freed the memory it references.
- Double free error.

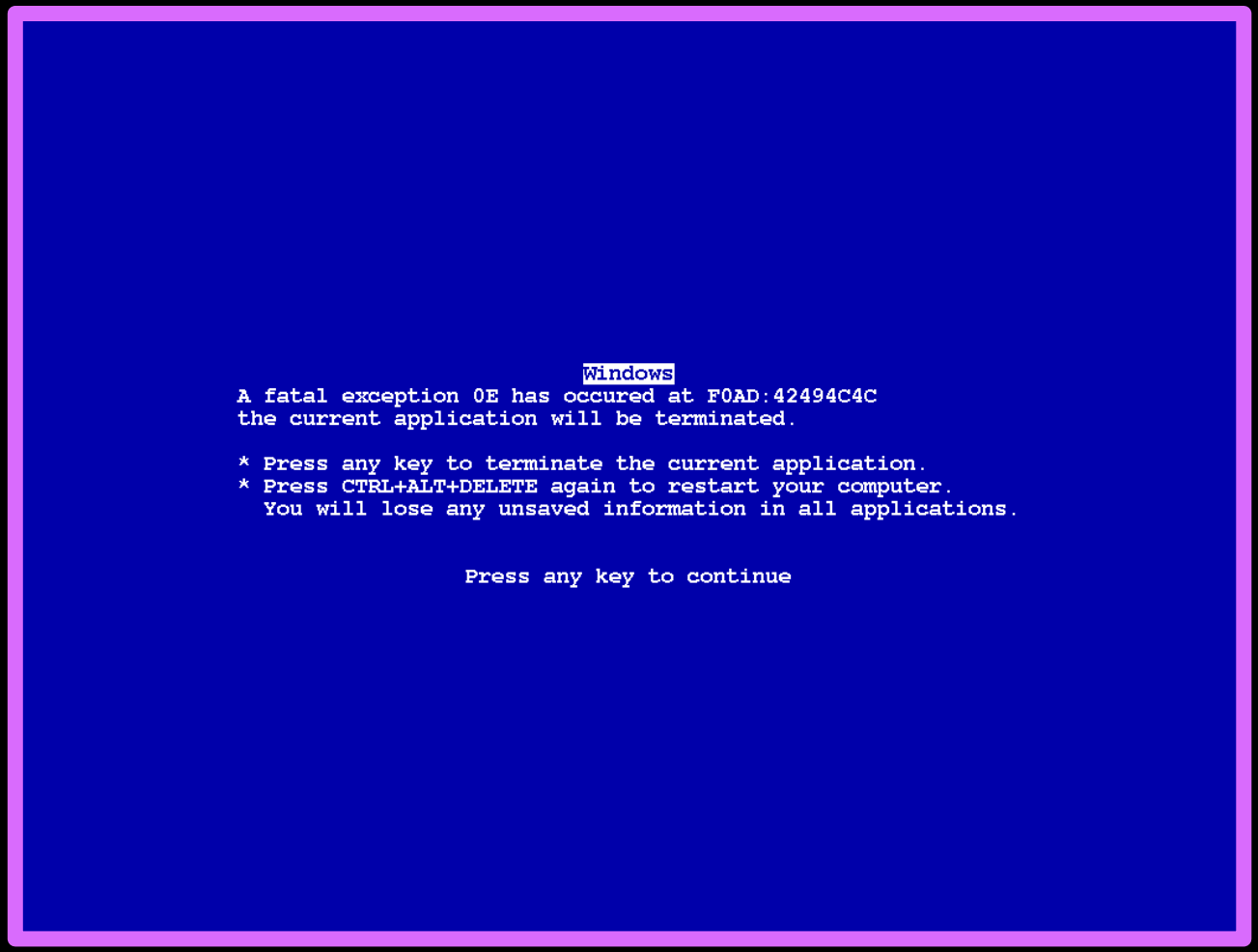
Multi-threading programming bugs
- Deadlock, where task A can't continue until task B finishes, but at the same time, task B can't continue until task A finishes.
- Race condition, where the computer does not perform tasks in the order the programmer intended.
- Concurrency errors in critical sections, mutual exclusions and other features of concurrent processing.

Interfacing bugs
- Incorrect API usage.
- Incorrect protocol implementation.
- Incorrect hardware handling.
- Incorrect assumptions of a particular platform.

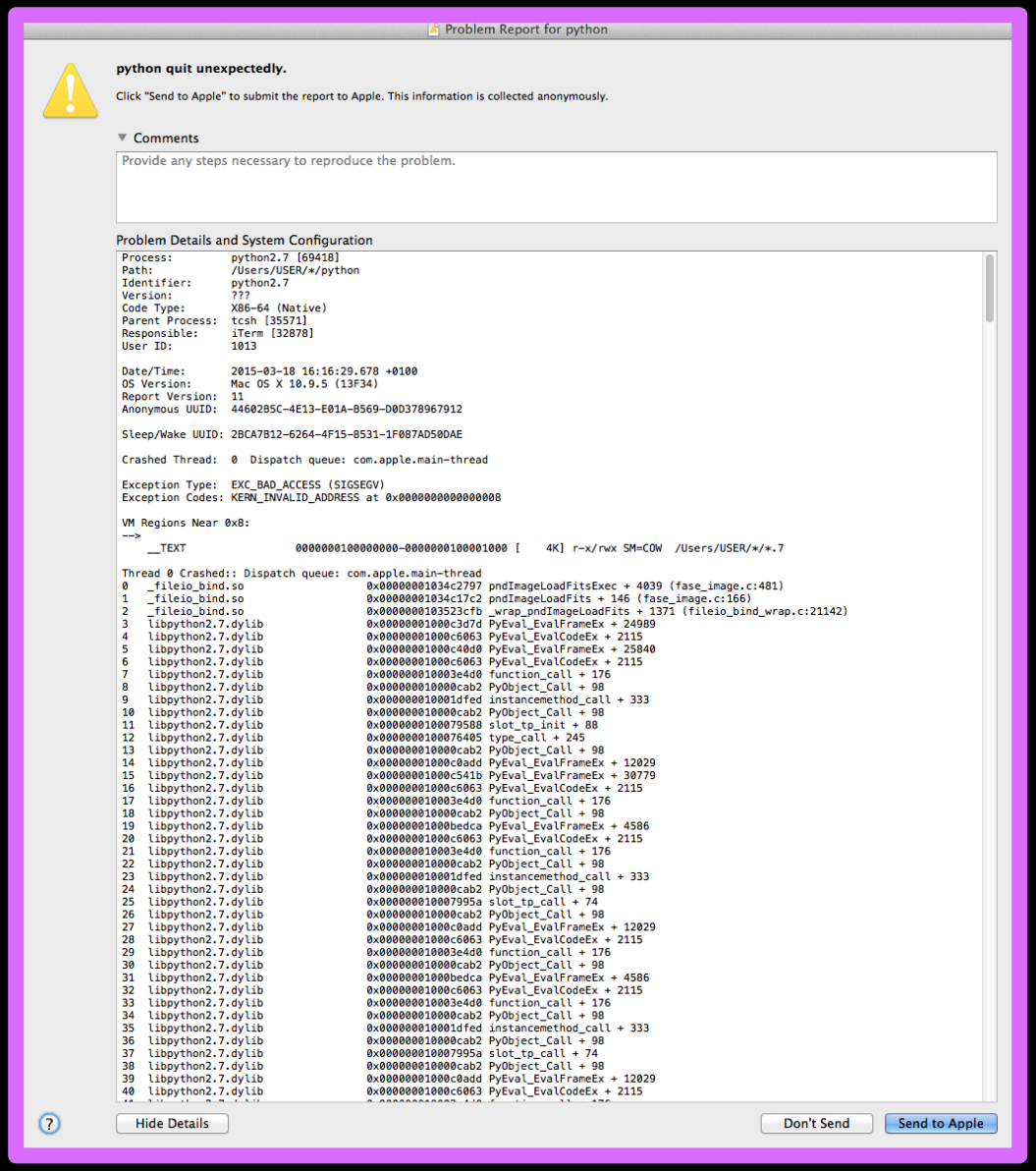
Performance bugs
- Too high computational complexity of algorithm.
- Random disk or memory access.

Teamworking bugs
- Unpropagated updates.
- Comments out of date or incorrect: many programmers assume the comments accurately describe the code.
- Differences between documentation and the actual product.

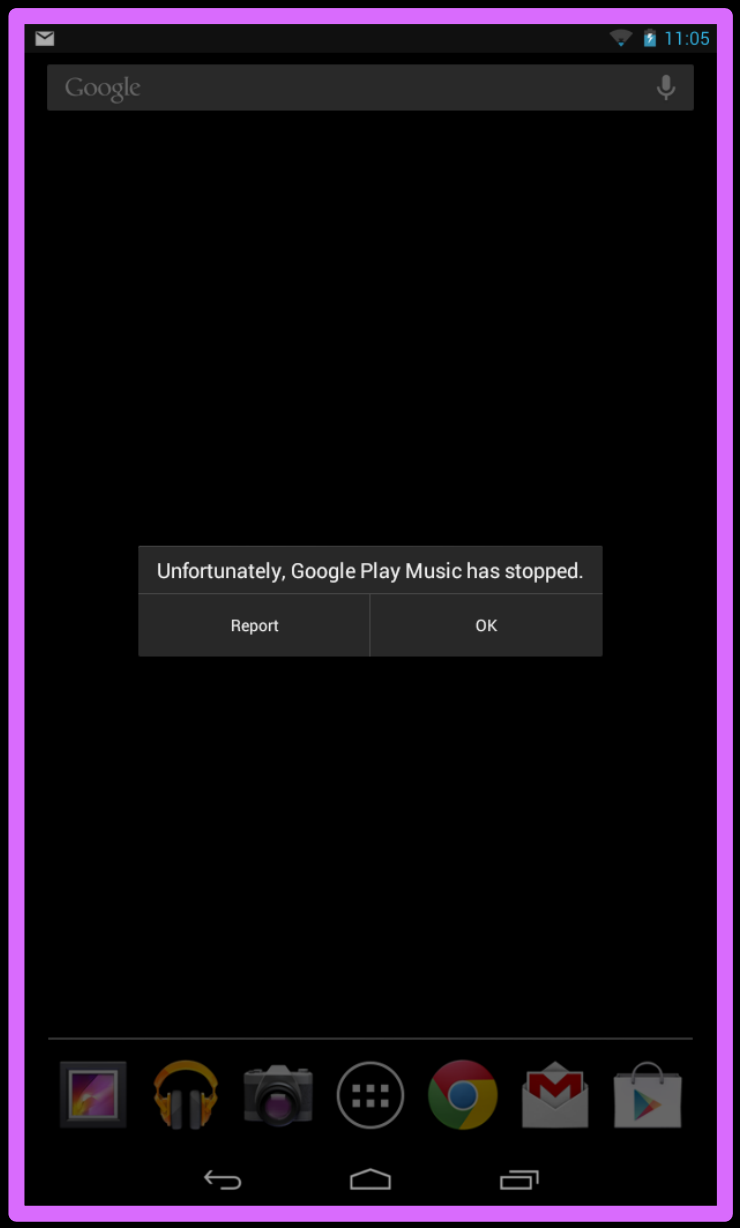
segmentation fault l'esercito



segmentation fault l'esercito



segmentation fault l'esercito

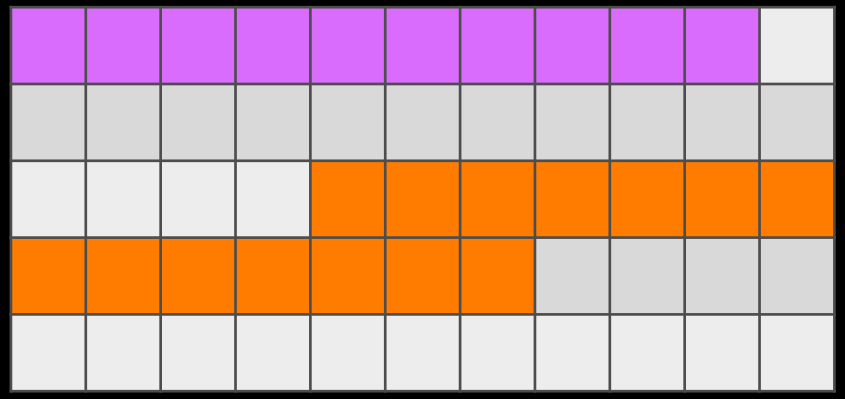


segmentation fault l'esercito

```
258408
258409
258410
258411
258412
258413
258414
258415
258416
258417
258418
258419
258420
258421
258422
258423
258424
258425
258426
258427
Segmentation fault
[meg] ~/Varia/Talks/asiesta_mar15 >
```

```c
#include <stdio.h>
#include <stdlib.h>


int main()
{
  int i;
  float *a;

  a=calloc(10,sizeof(float));

  for(i=0; i<1000000; i++) {
    a[i]=1;
    printf("%d\n", i);
  }


  return 0;

}
```

memoria



overflow l'esercito

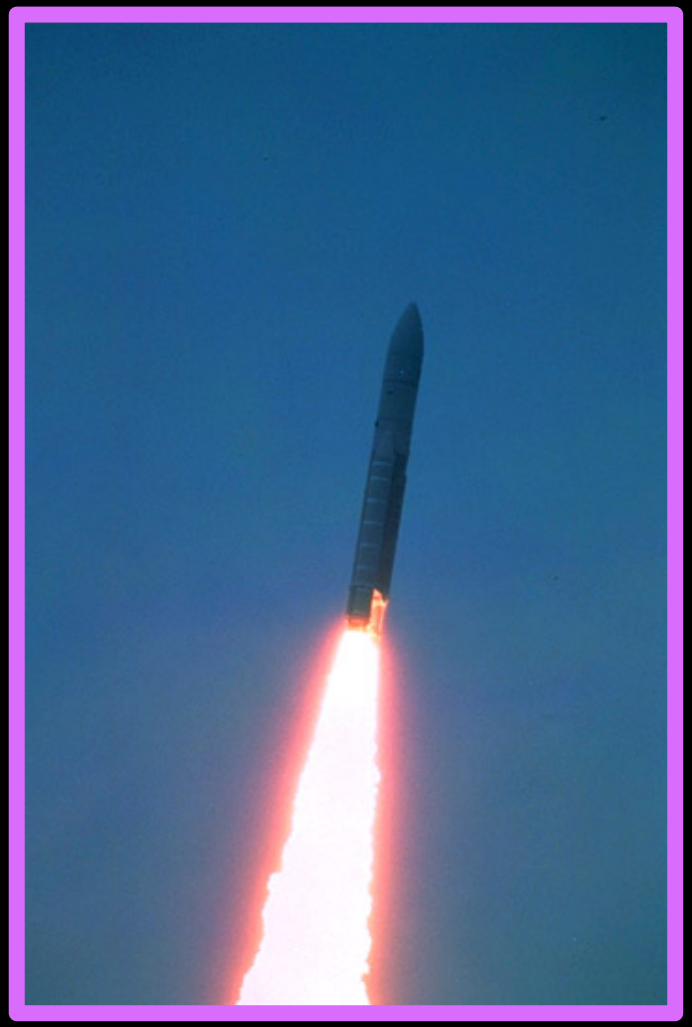
```c
#include <stdio.h>


int main()
{

  char a=0;

  printf("Variable size is %lu byte\n", sizeof(char));

  a=127;

  printf("a=%d\n", a);

  a=200;

  printf("a=%d\n", a);

  return 0;

}
```

```
[meg] ~/Varia/Talks/asiesta_mar15 > ./over
Variable size is 1 byte
a=127
a=-56
[meg] ~/Varia/Talks/asiesta_mar15 >
```

overflow l'esercito

June 4, 1996, Ariane 5 maiden flight.

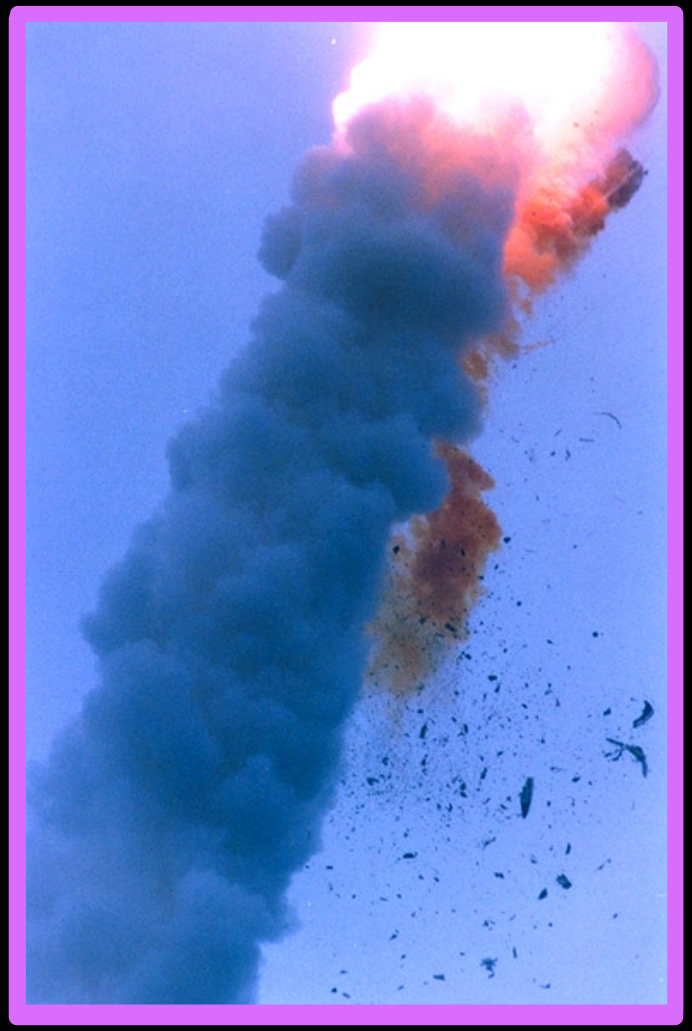
Shortly after launch, the guidance software tried to convert the horizontal velocity (which was greater in the Ariane 5 than in the Ariane 4) from a 64-bit floating point number to a 16-bit signed integer, which caused an overflow error. The guidance system (and its backup, which had the same bug) then shut down, causing the rocket to veer off-course and, ultimately, self destruct 30 seconds after launch.



overflow l'esercito

June 4, 1996, Ariane 5 maiden flight.

Shortly after launch, the guidance software tried to convert the horizontal velocity (which was greater in the Ariane 5 than in the Ariane 4) from a 64-bit floating point number to a 16-bit signed integer, which caused an overflow error. The guidance system (and its backup, which had the same bug) then shut down, causing the rocket to veer off-course and, ultimately, self destruct 30 seconds after launch.



overflow l'esercito

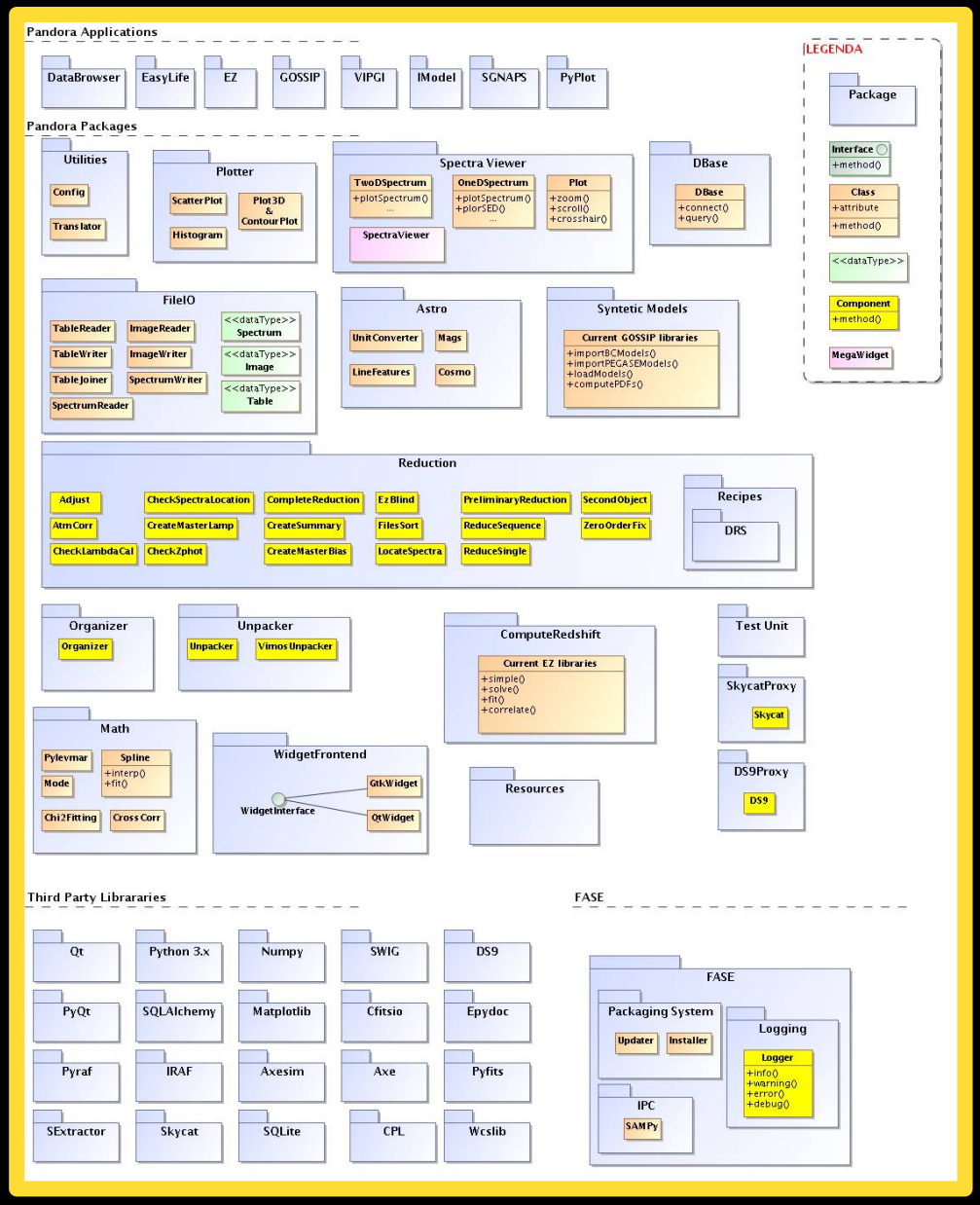
```
#!/usr/bin/env python

a=127
print a, "a is %s" % type(a).__name__

a=1e27
print a, "a is %s" % type(a).__name__
```

```
[meg] ~/Varia/Talks/asiesta_mar15 > ./over.py
127 a is int
1e+27 a is float
[meg] ~/Varia/Talks/asiesta_mar15 >
```

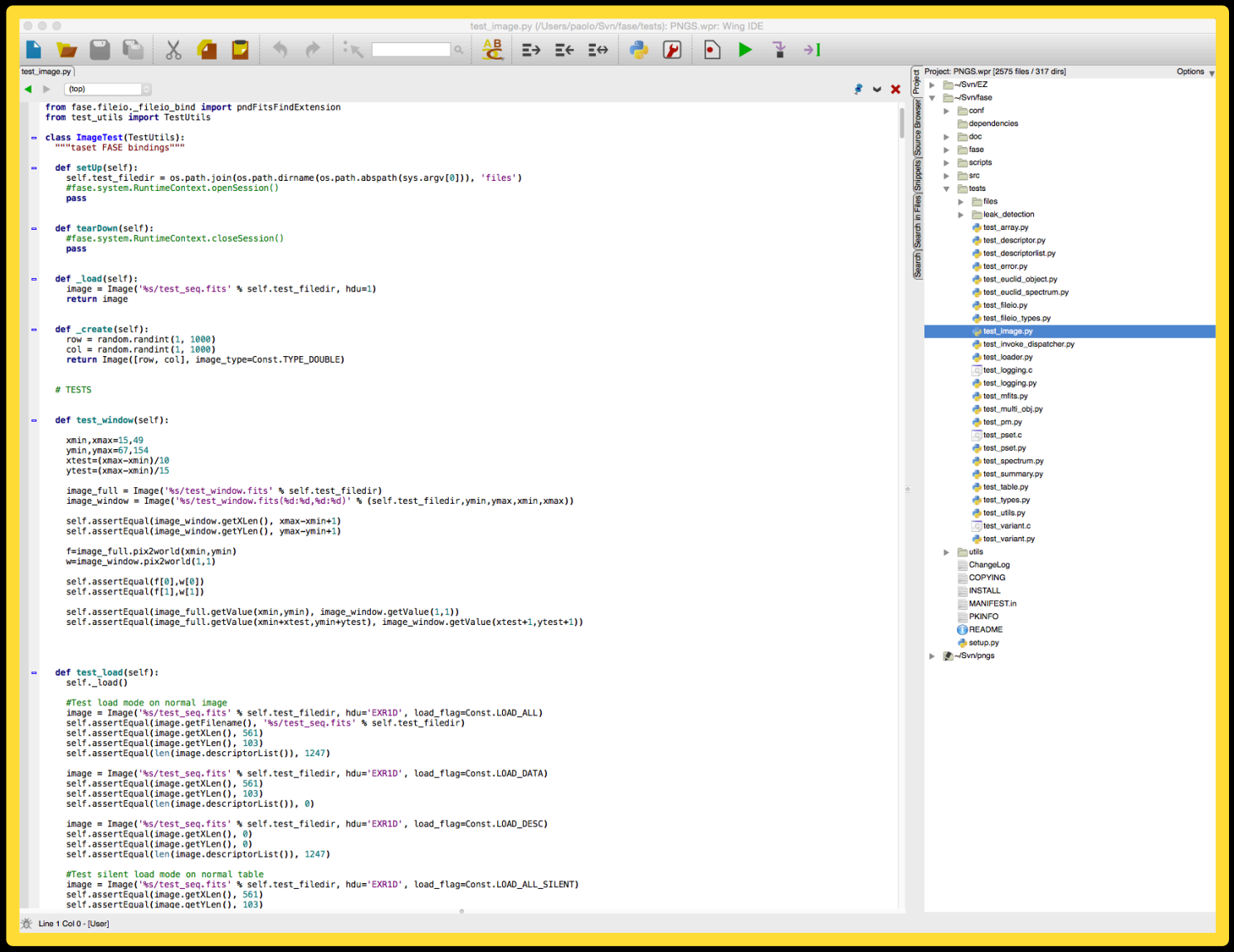
le armi

come combattere i *bugs*

progettazione le armi



unit tests le armi



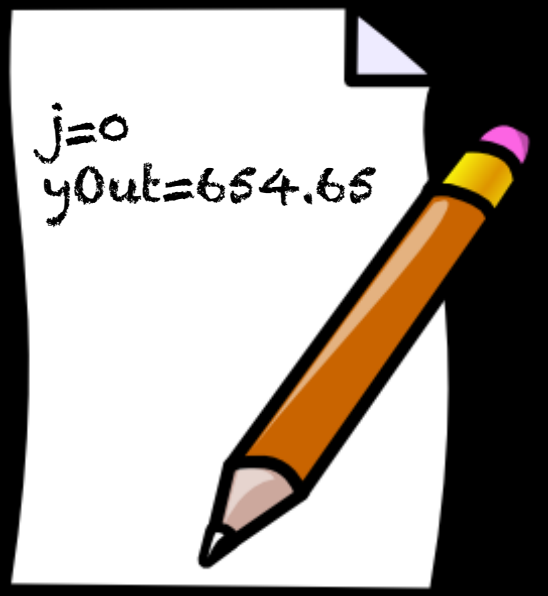
memory check le armi

debugger le armi

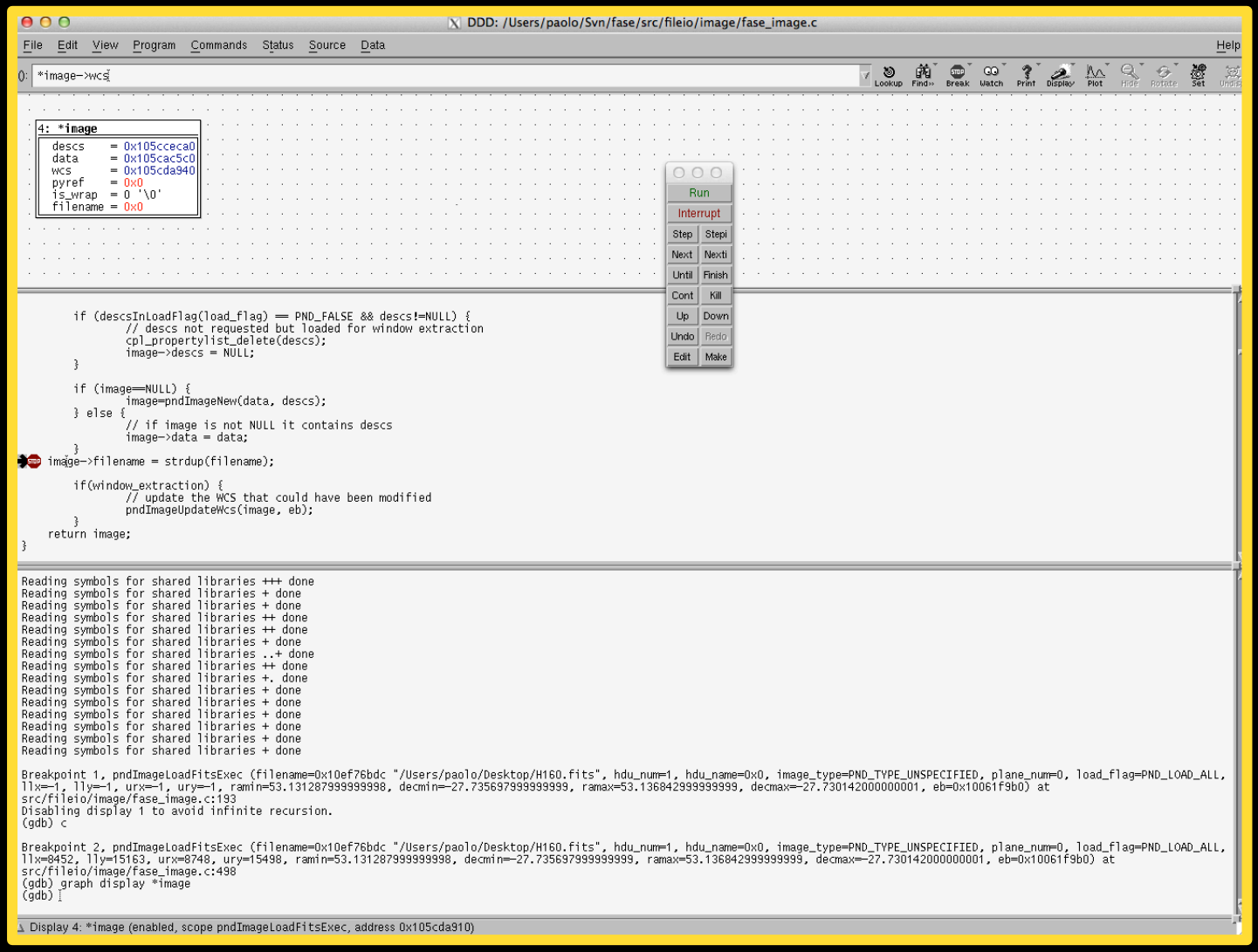
VmSpDerDisp.c

```
if (tunedModel)
    deleteDistModel1D(tunedModel);


/* COPY DIST. MODEL */
/* creat new model */
tunedModel = newDistModel1D(slit->invDis[i]->order);
/* copy offset */
tunedModel->offset = slit->invDis[i]->offset;
/* copy coefficients */
for(j=0; j<=slit->invDis[i]->order; j++)
    tunedModel->coefs[j] = slit->invDis[i]->coefs[j];

/* extract spectrum for this row */
for (j = -nPixBelow; j <= nPixAbove; j++) {
    /* compute Y-CCD-pixel of spectrum */
    yOut = slit->ccdY->data[i] + j;
    /* compute X-pixel of spectrum */

    /* ALEX 29/10/03: if crvPol coefs = 0.0 then always use crvPol[0]:
       (crvPol[i] = 0.0) happens for central columns of a spectrum
       if global models have not been set */
    if (noGlobalModel) {
        xOutF =slit->ccdX->data[i] + computeDistModel1D(slit->crvPol[0],
                yOut);
    } else {
        xOutF =slit->ccdX->data[i] + computeDistModel1D(slit->crvPol[i],
                yOut);
    }


    printf("%d %f\n", j, yOut);


    xOut = xOutF;  /* Make it integer (truncation) */
    if (xOut >= 0 && xOut+1 < imageXlen) {
        if (yOut >= 0 && yOut < imageYlen) {
            /* simple linear interpolation */
            frac = xOutF-xOut;
            datVal= ( (1.0-frac)*inputImage->data[xOut + yOut*imageXlen] +
                      frac*inputImage->data[xOut+1+yOut*imageXlen] );
        } else {
            /*
             *  Fill with zeroes parts of the spectrum dispersed beyond
             *  the CCD frame.
             */
            datVal = 0.;
        }
        /* store in bufferUseful */
        spectrum->data[nPixBelow+j] = datVal;
    } else {
        /*
                          *  Mark as invalid the part of the slit extending beyond the
```

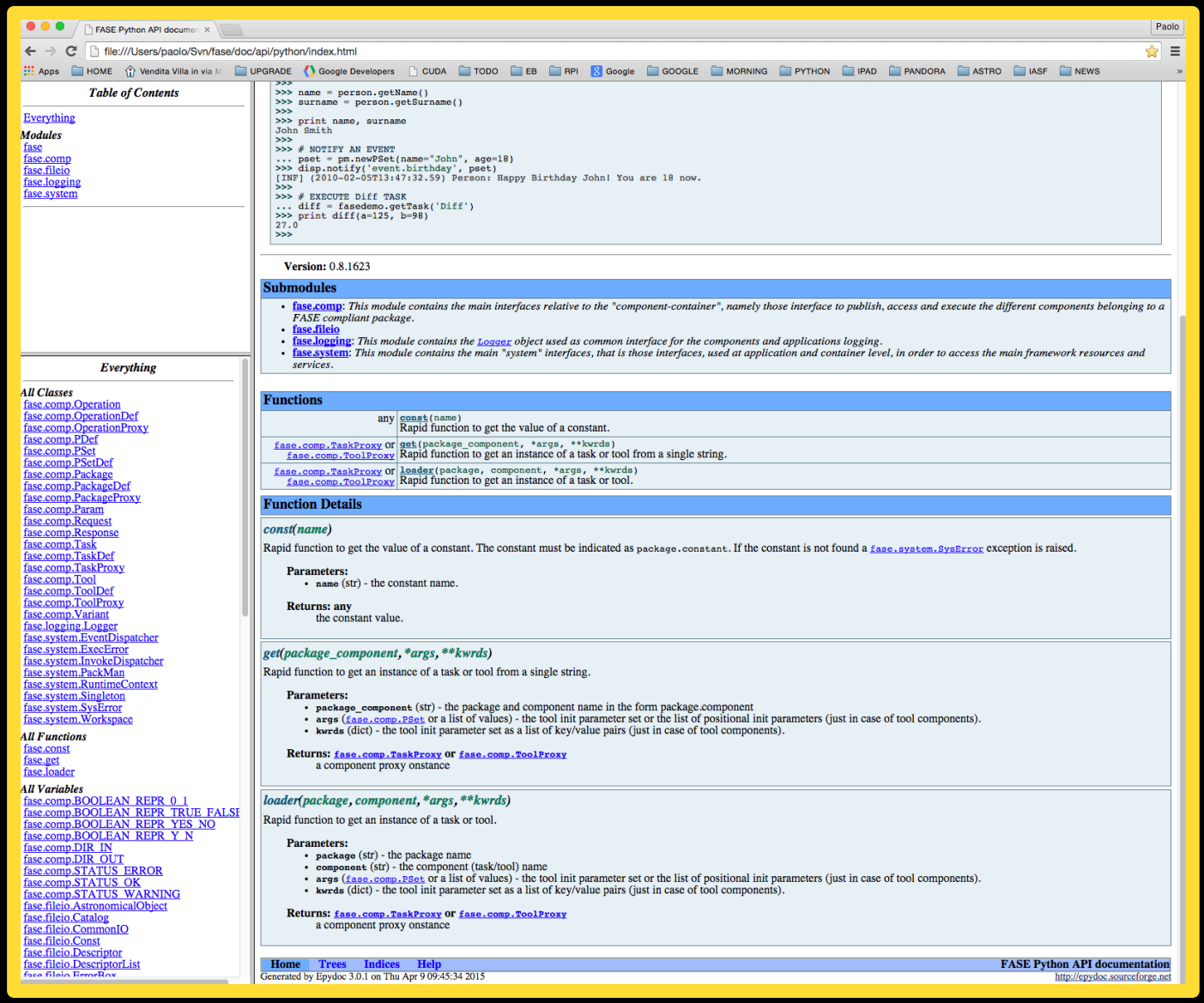
-:--- VmSpDerDisp.c 67% L463 (C/l Abbrev)



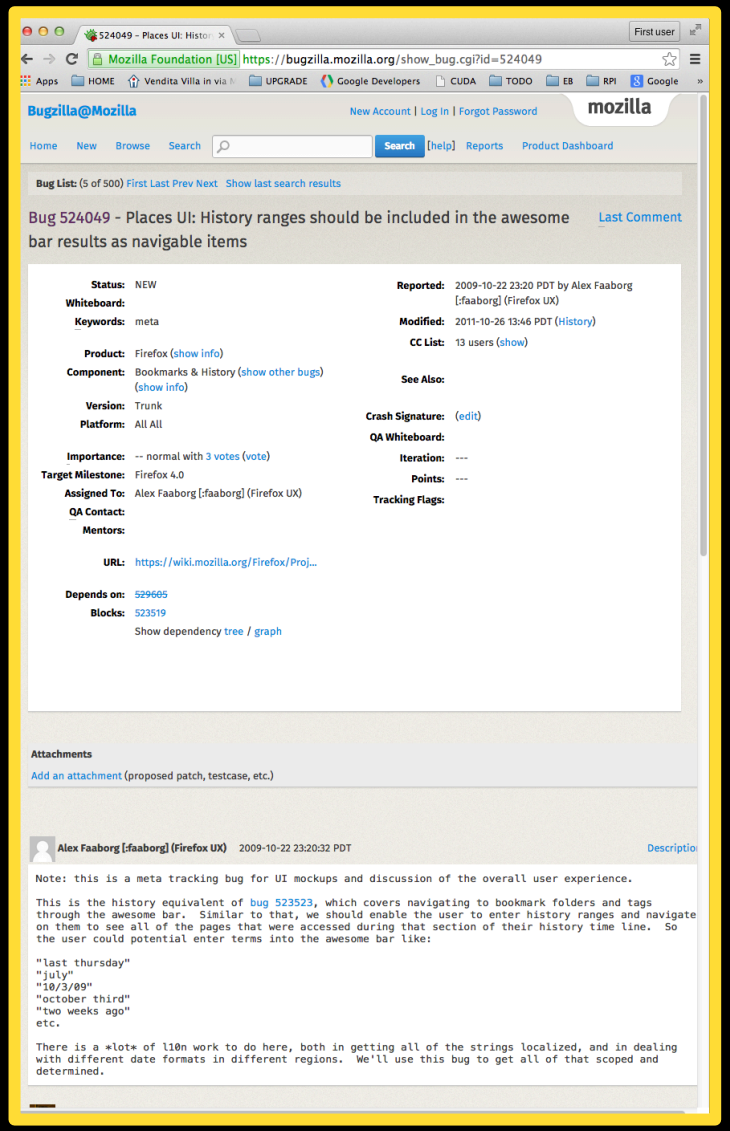
debugger le armi



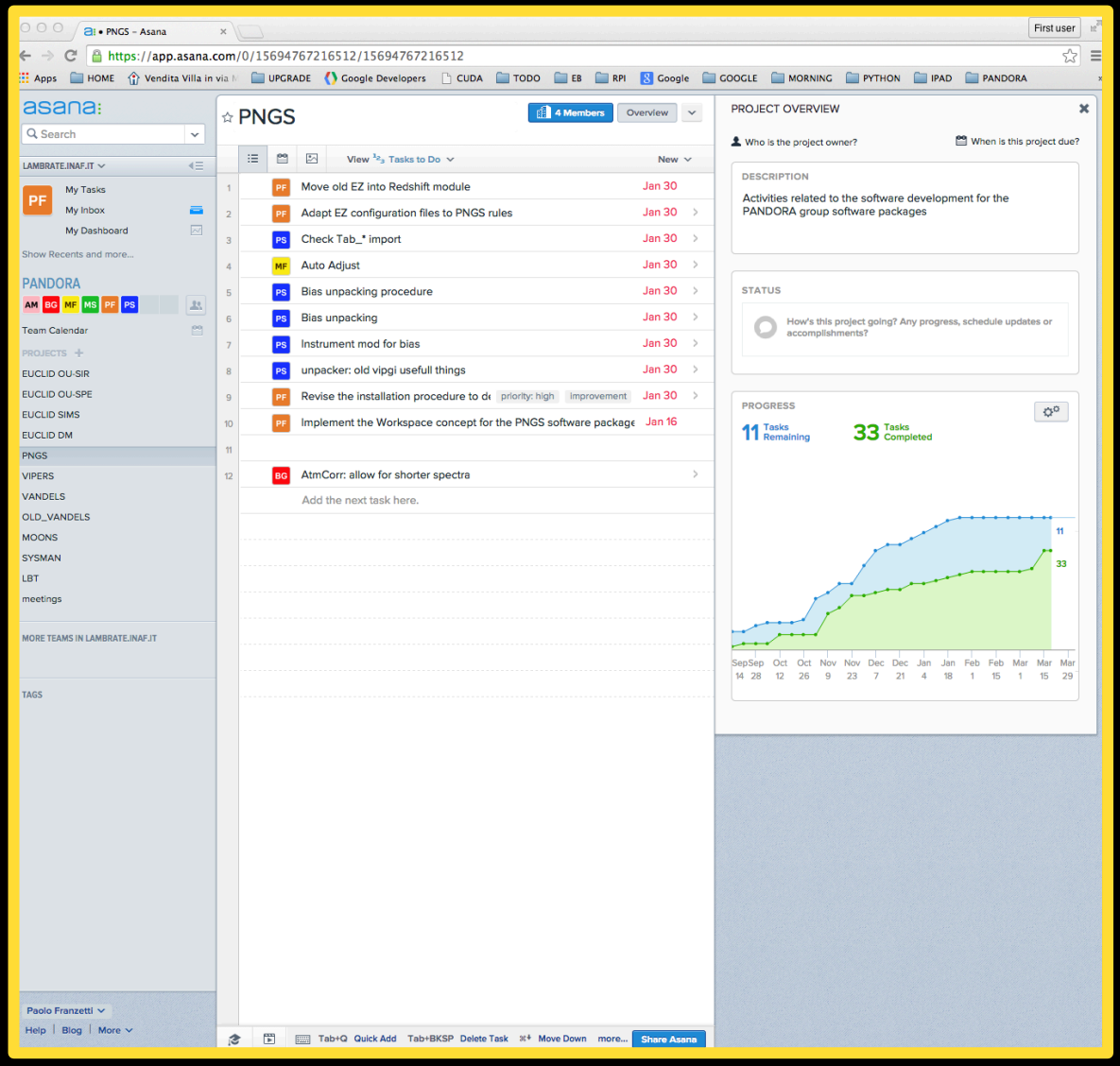
documentazione le armi



tracking le armi



tracking le armi



la caccia

Ogni mattina allo IASF un bug si attiva
e sa che dovrà correre più del programmatore o verrà fissato.
Ogni mattina allo IASF, un programmatore timbra
e sa che dovrà correre più del bug o verrà licenziato.

Tecnologo anonimo

1 / scoperta la caccia

1. **Scoperta**
   - ✓ **Subito prima di una release**
   - ✓ **10 minuti dopo una release**
   - ✓ **Appena detto a Bianca: “OK funziona, provalo”**

2 / incredulità la caccia

1. **Scoperta**
2. **Incredulità**
   - ✓ **Come ha fatto a funzionare finora ?**
   - ✓ **È impossibile (L. Paioro)**

3 / diffusione la caccia

1. Scoperta
2. Incredulità
3. Diffusione

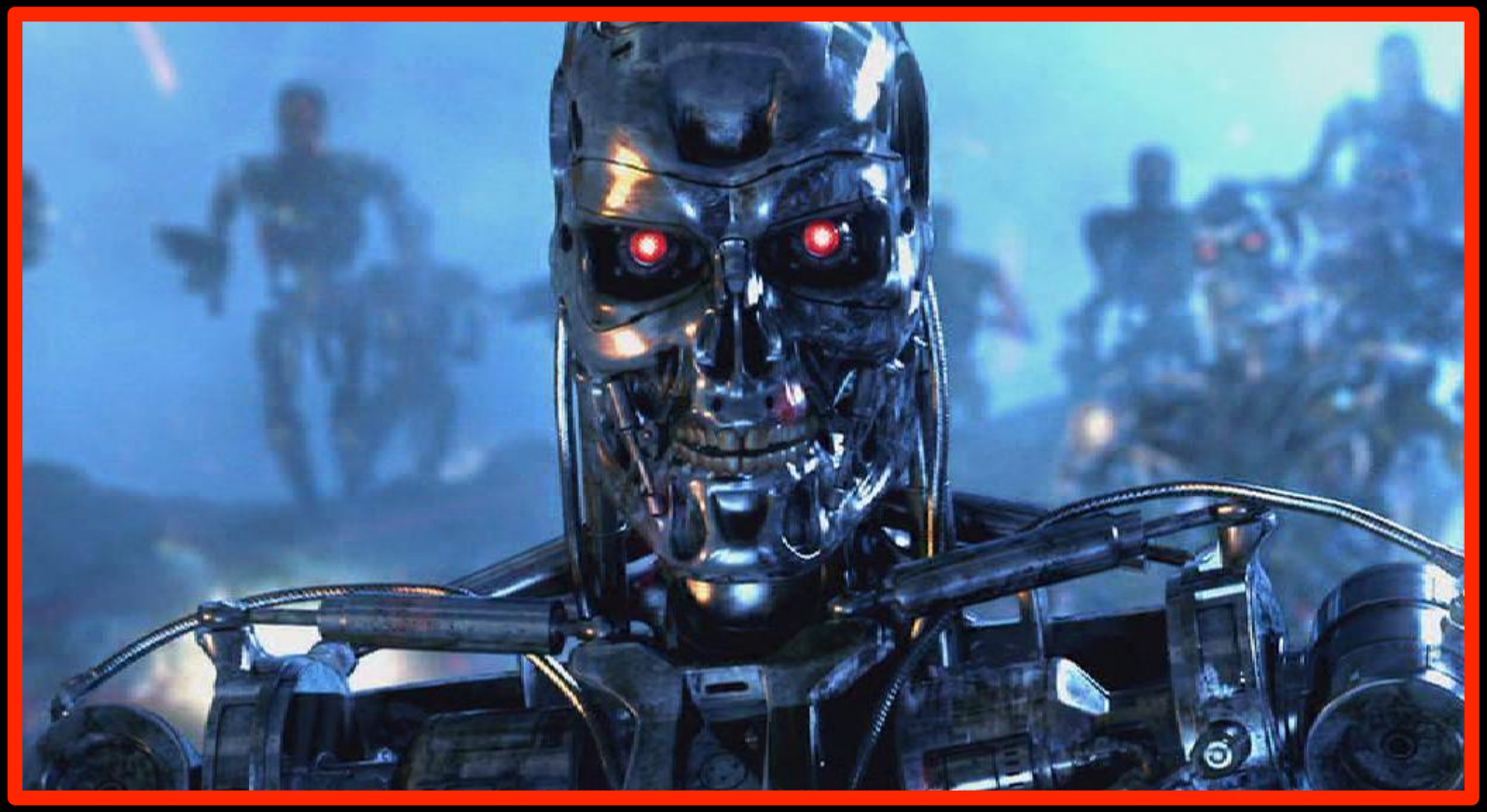
4 / pessimismo la caccia

1. **Scoperta**
2. **Incredulità**
3. **Diffusione**
4. **Pessimismo**
   - ✓ **Non ne usciremo mai …**

5 / soluzione la caccia

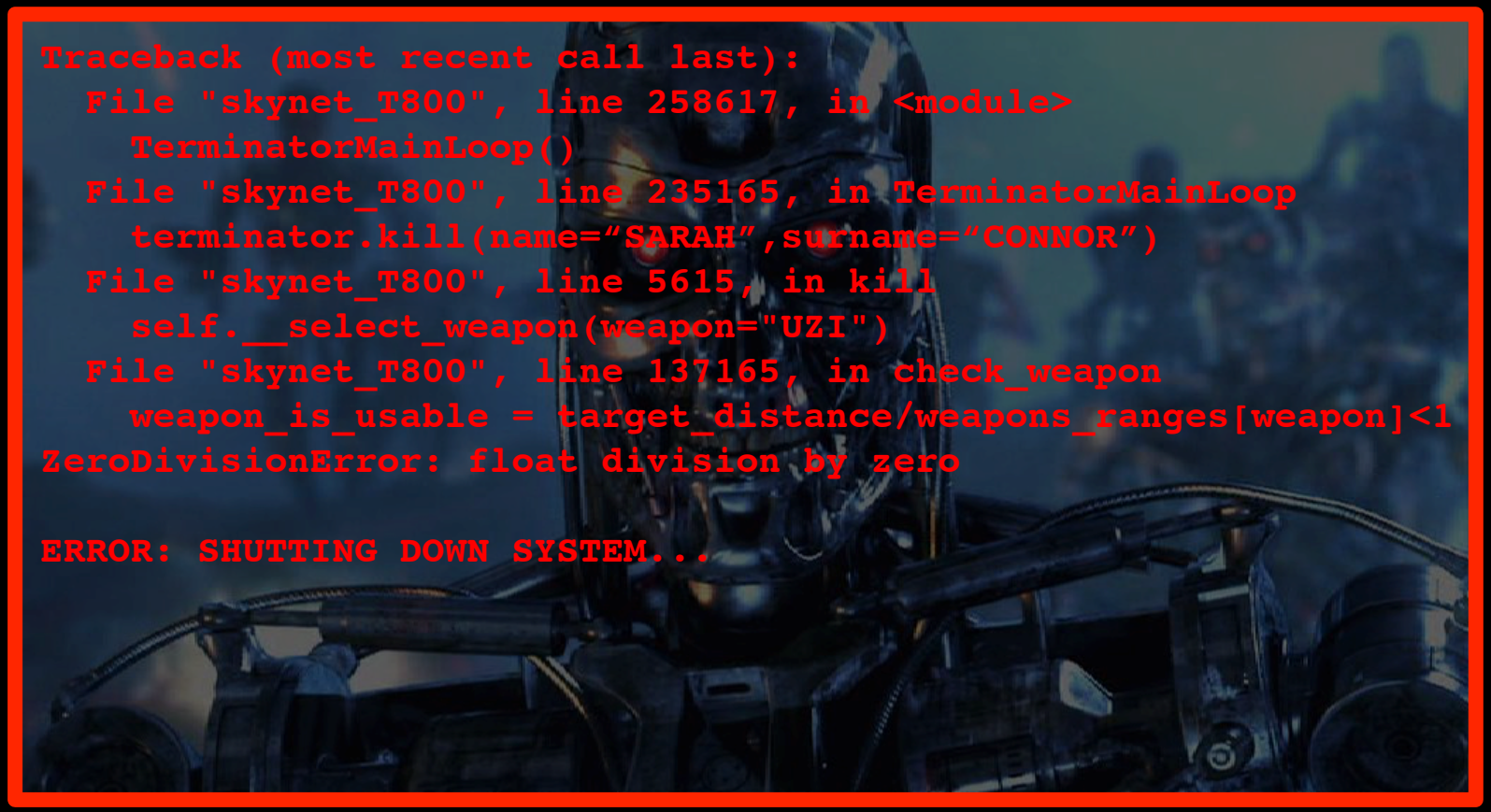
1. Scoperta
2. Incredulità
3. Diffusione
4. Pessimismo
5. Soluzione

concludendo



concludendo

… corri, nasconditi e aspetta



```
Traceback (most recent call last):
  File "skynet_T800", line 258617, in <module>
    TerminatorMainLoop()
  File "skynet_T800", line 235165, in TerminatorMainLoop
    terminator.kill(name="SARAH",surname="CONNOR")
  File "skynet_T800", line 5615, in kill
    self.__select_weapon(weapon="UZI")
  File "skynet_T800", line 137165, in check_weapon
    weapon_is_usable = target_distance/weapons_ranges[weapon]<1
ZeroDivisionError: float division by zero

ERROR: SHUTTING DOWN SYSTEM...
```