

FRAMA-C DAY 2016

# KEYNOTE: HOW FRAMA-C CAN HELP A VERIFICATION & ASSESSMENT BODY

F. SADMI

2016/06/20



**BUREAU  
VERITAS**

# Dependability

Ability to provide services that can defensibly be trusted within a time-period.



# A tradeoff ...

Cost

Customer

Standards

Planning

Security / Safety

Availability

Man Power

Performance

Maintenability

Reliability

Dependability

=

RAMS

Oil & Gas



Process



(Renewable) Energy & Nuclear &



Automotive



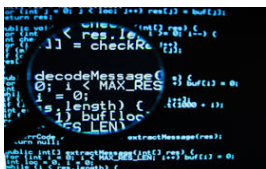
AERO / Defense



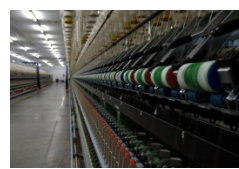
Railway



Software & PLC



Manufacturing



Product / Process  
Industrial Control system  
Dependability / Safety

Safety Functions

Sensors

Logic

Actuators

Different standards / referentials  
IEC 61508 / IEC 61511 / IEC 61513 / RCC-E  
ISO 13849 / ISO 26262 / DO 178C  
CENELEC 5012x / OQA / ISA  
HIPS & BV-SW-100

## ▶ Product:

- Identification of the functionalities and the technical perimeter

## ▶ Referential:

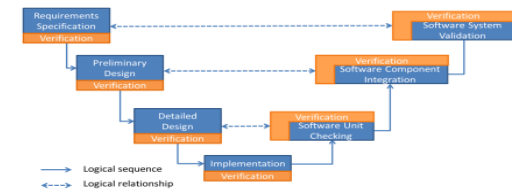
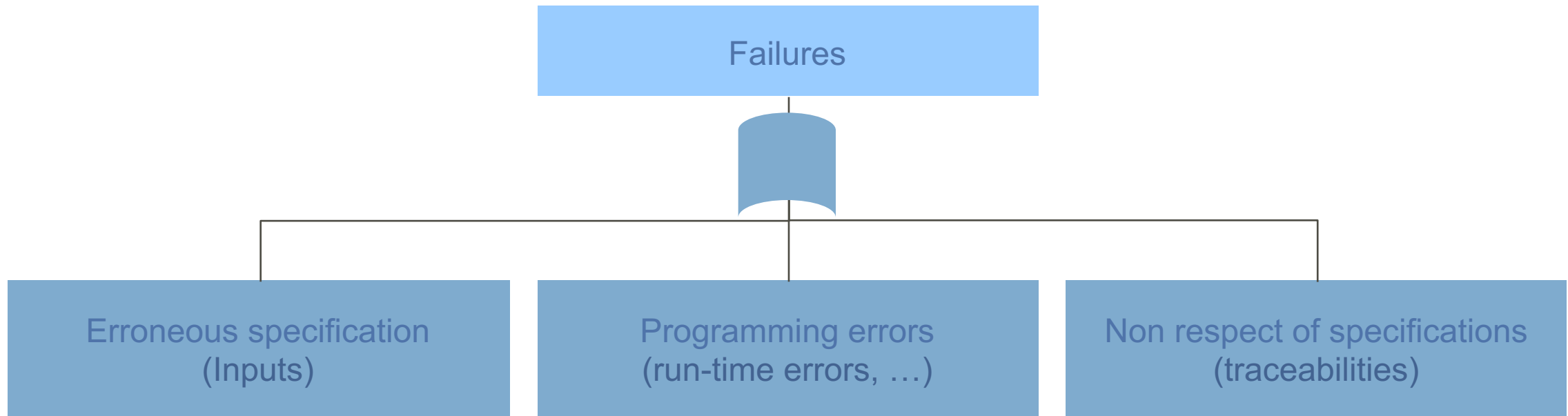
- List of requirements

## ▶ Assessment:

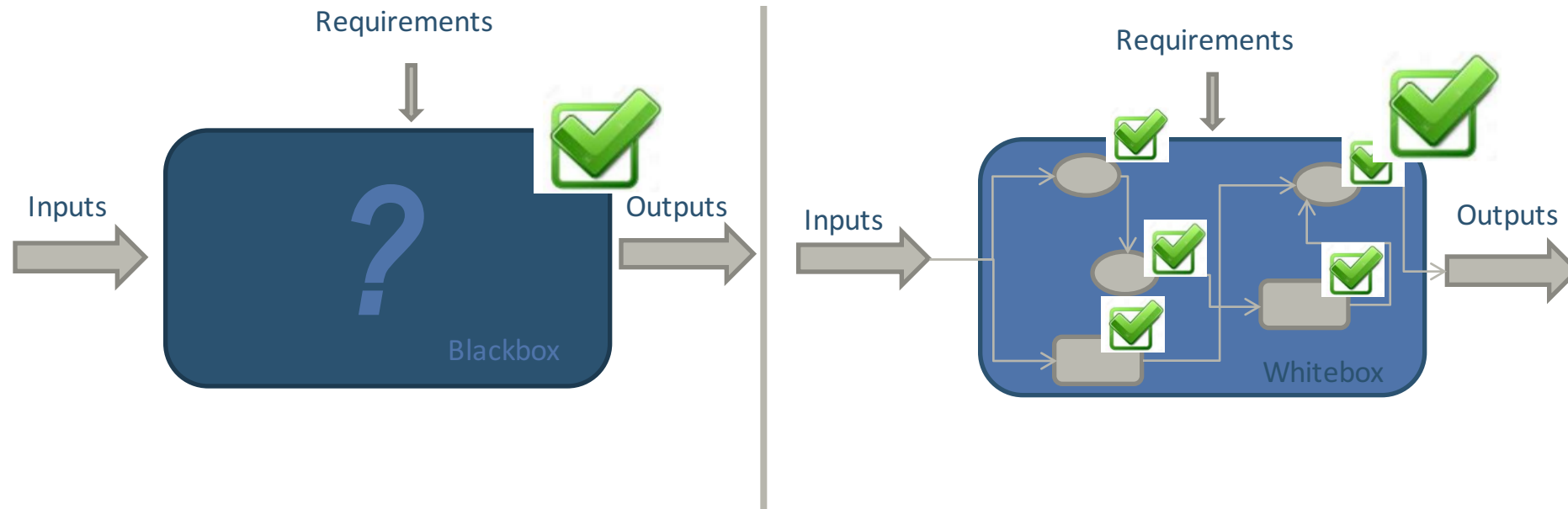
- Documentation assessment (specification, tests, code, ...)
- Process assessment (audit)

## ▶ Results:

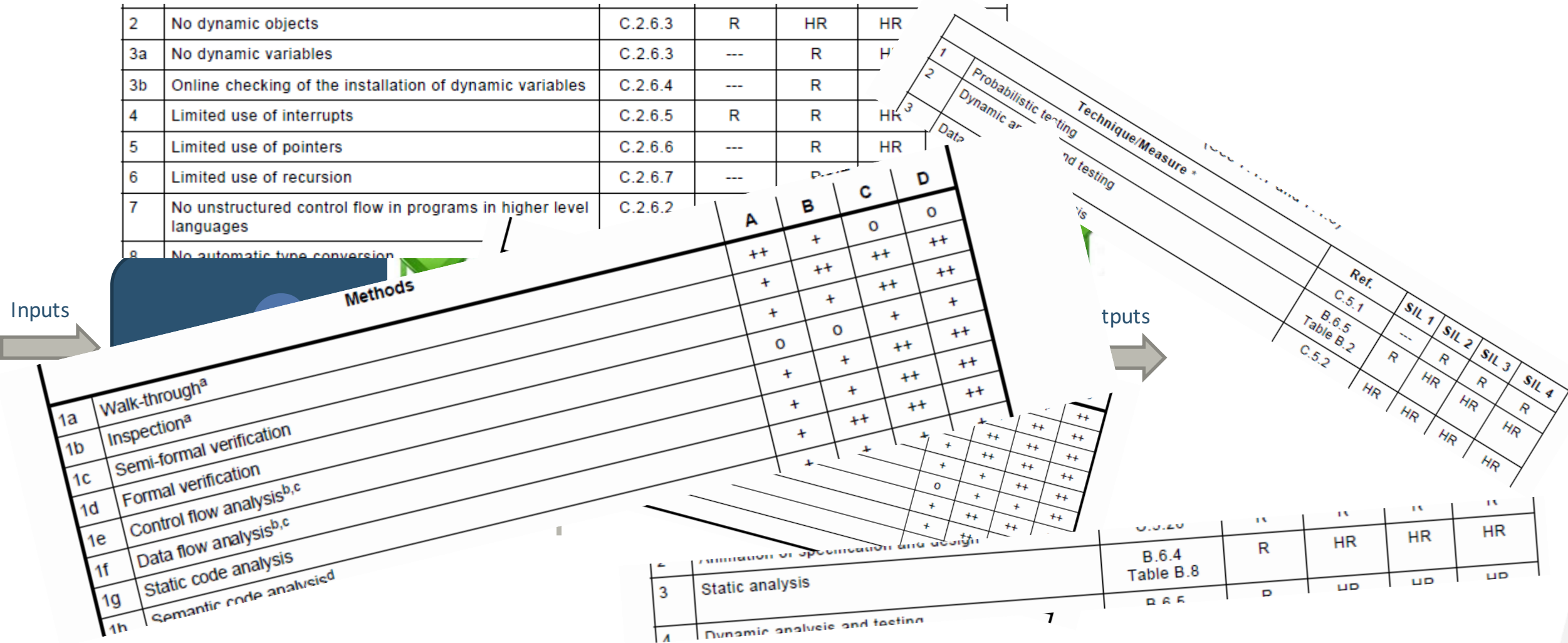
- Certificate



# Software verifications (required by standards)



# Software verifications (required by standards)





# How to comply with those requirements

Demonstration based on :

- ▶ Manual means
- ▶ Automatic means



Quality of the evidence?

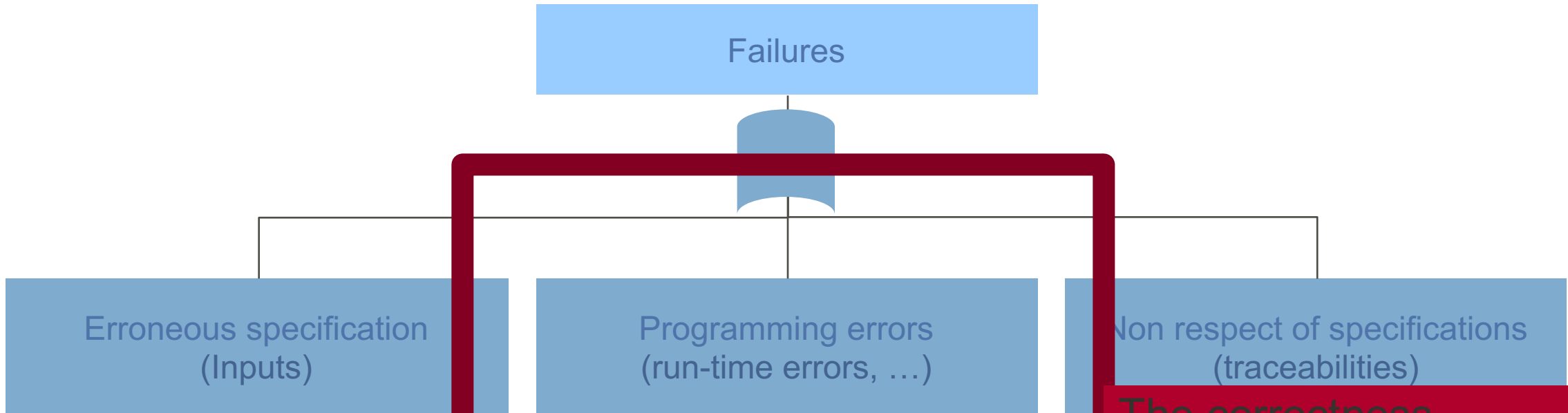
Quid of :

- ▶ The correctness?
- ▶ The exhaustiveness / soundness ?
- ▶ The recordings and verification?



Does the mean used by the customer achieves the objective ?

- ▶ For the coding rules
- ▶ For the naming rules
- ▶ For the run time errors
- ▶ ...



Review / Inspection



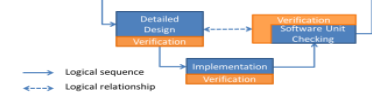
Code analysis



The correctness  
The exhaustiveness / soundness  
The recordings and verification



```
private #user;  
private #password;  
private #database;  
private #charset;  
static public #link = null;  
static public function Connect()  
{  
    #link = mysql_connect(#host,#username,  
        #password);  
    if (!$link) {  
        #error = mysql_error();  
        return false;  
    }  
    mysql_select_db(#database, $link);  
    mysql_query("SET CHARACTER SET #charset");  
    return $link;  
}
```



Each programming language has possible programming errors:

- ▶ Division by 0
- ▶ Dead code
- ▶ Buffer overflow
- ▶ Out of bound accesses
- ▶ Dangerous cast
- ▶ Non initialized variables
- ▶ ...



Found by Frama-C

# How do we work with Frama-C

- ▶ Cross acceptance of Frama-C results
  - Easy to check the configuration of the customer
  - Verify only the results
  
- ▶ Double checking of the customer results
  - In case of doubt, possibility to run Frama-C to challenge customer results

- ▶ Skills improvement
- ▶ Gain of time if Frama-c is used by the customer
- ▶ To be in capacity to run independent analysis



Automate systematic analyses to keep the focus on specific analyses

(& ensure that your tools achieve yours goals)



Operational Excellence

## Equipment Status Board



**ALL  
ACCIDENTS  
NO MATTER  
HOW MINOR  
MUST BE  
REPORTED  
TO YOUR  
SUPERVISOR**



**BUREAU  
VERITAS**

***Move Forward with Confidence***