

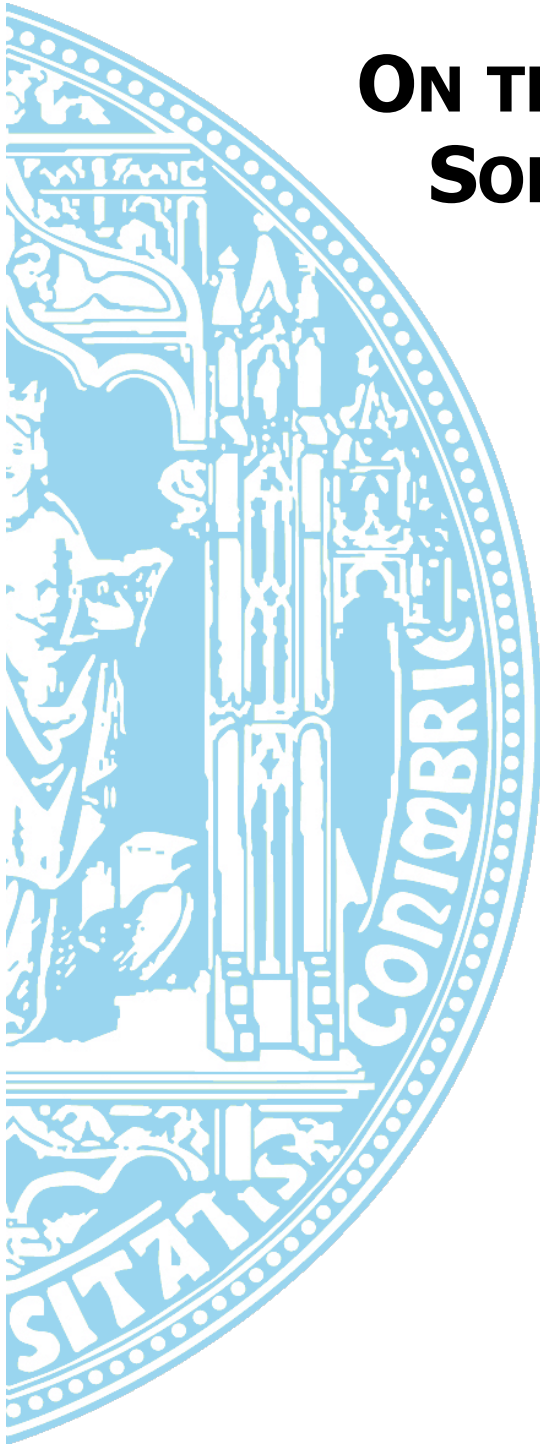
ON THE RELEVANCE OF ISVV FOR AEROSPACE SOFTWARE **OR** REAL ISSUES IN AEROSPACE CRITICAL SYSTEMS DEVELOPMENT

N. Silva U. of Coimbra/CSW, Portugal
M. Vieira U. of Coimbra, Portugal

IFIP WG 10.4
68th Meeting
Búzios, Brazil
June 28th, 2015

Marco Vieira
mvieira@dei.uc.pt

Department of Informatics Engineering
University of Coimbra - Portugal






CONTEXT

Space safety critical systems' development follows strict processes, ruled by standards (i.e. ECSS)

- Verifications performed to reduce defects
- **Independent Software Verification & Validation (ISVV)** aims at finding remaining defects
 - Performed by an independent entity
 - Includes a multitude of different techniques
 - Addresses the multiple artifacts of the project
 - Requirements Verification
 - Design Verification
 - Code Verification
 - Test Verification
 - ...



STANDARDS AND MORE STANDARDS...

Misc	Automotive	Automation	Railway	Airborne	Space
IEC 61508 <i>Functional safety of electrical/electronic/programmable electronic safety-related systems</i>				ARP 4761 <i>Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment</i>	ECSS series <i>Processes for project management, engineering and product assurance in space projects and applications</i>
IEC 62304 <i>Medical device software – Software life cycle processes</i>	ISO 26262 <i>Road vehicles - Functional safety</i>	IEC 61511 <i>Functional safety - Safety instrumented systems for the process industry sector</i>	EN 50126 <i>Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS)</i>	ARP 4754 <i>Certification Considerations for Highly-Integrated or Complex Aircraft</i>	NASA-STD-8719.13B <i>Software Safety Standard - NASA</i>
IEC 60880 <i>Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions</i>		IEC 62061 <i>Safety of machinery - Functional safety of electrical, electronic and programmable electronic control systems</i>	EN 50128 <i>Railway applications - Communication signalling systems - railway control protection</i>		
			EN 50129 <i>Railway applications - Communication signalling systems - electronic signalling</i>		

Are Standards Enough?

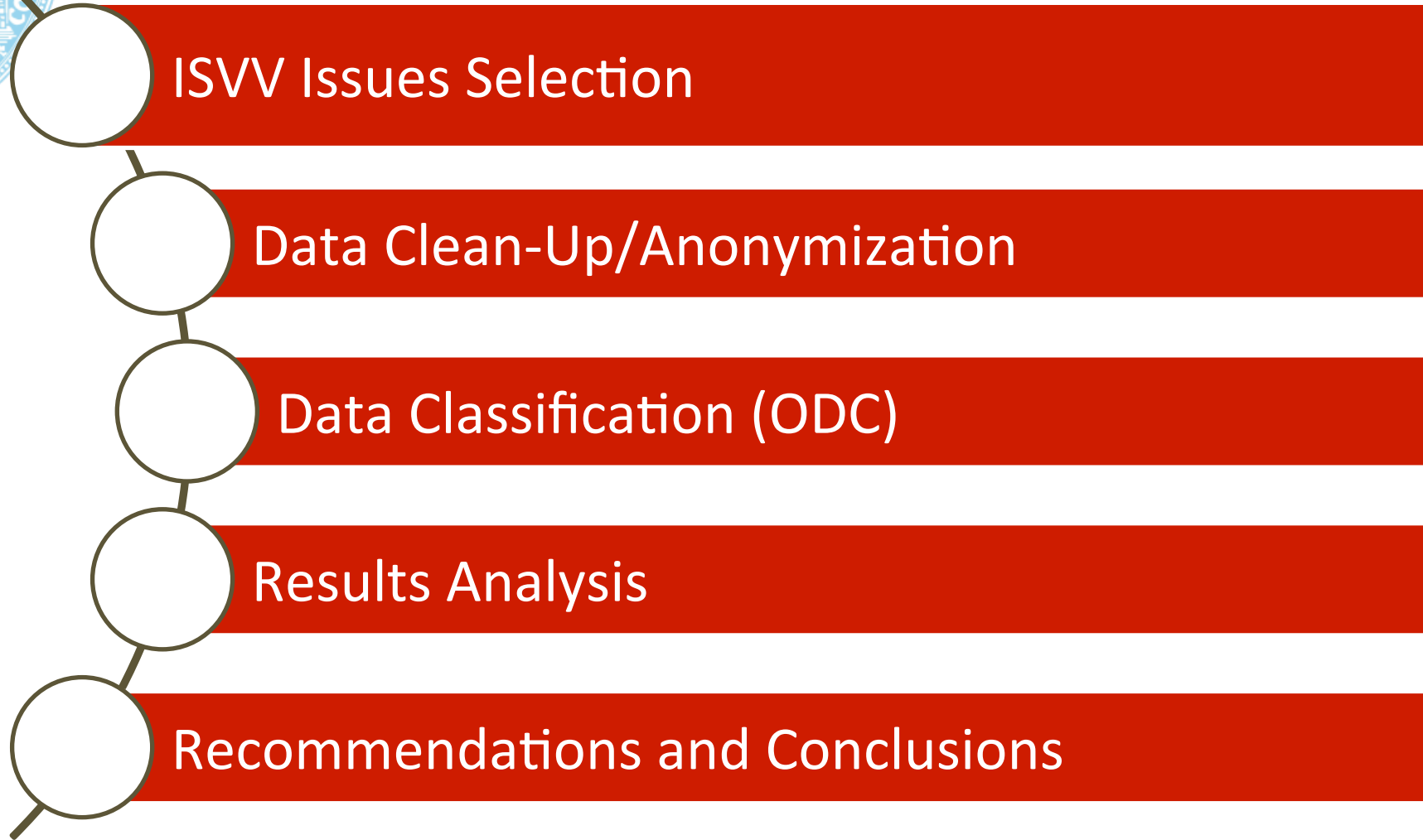


GOALS OF THE STUDY

Focus on Aerospace Critical Systems development

- **Goal 1:** Understand the relevance of ISVV
- **Goal 2:** Analyze real issues in aerospace critical systems development
- **Goal 3:** Study the applicability of ODC to classify issues
 - ODC is widely used to classify issues that belong to the software development phases
 - Defect Type, Defect Trigger, Defect Impact
 - Defines attributes according to which issues can be classified
 - Allow for statistical and root-cause analysis

OVERALL APPROACH



THE SYSTEMS



- Related to the space domain (satellite systems)
 - Cover different types of systems
 - Start-up or boot software, on-board application software, payload software, full system
 - 16 different systems or subsystems
 - Analysis of more than 10000 requirements, more than 1 million LoC, and over 1.500 tests
- The engineering processes used for the selected missions had to follow the ECSS standards
 - Similar lifecycle and strict requirements imposed by European Space Agency (ESA)
- **Anonymous... for reasons you understand!**



ISSUES ANALYZED

Detection Phase	Amount of RIDs
Requirements Verification	162
Design Verification	112
Code Verification	378
Test Verification	398
Ground Monitoring	20
Total	1070

14% classified as major issues, 66% as minor and 20% as improvement comments

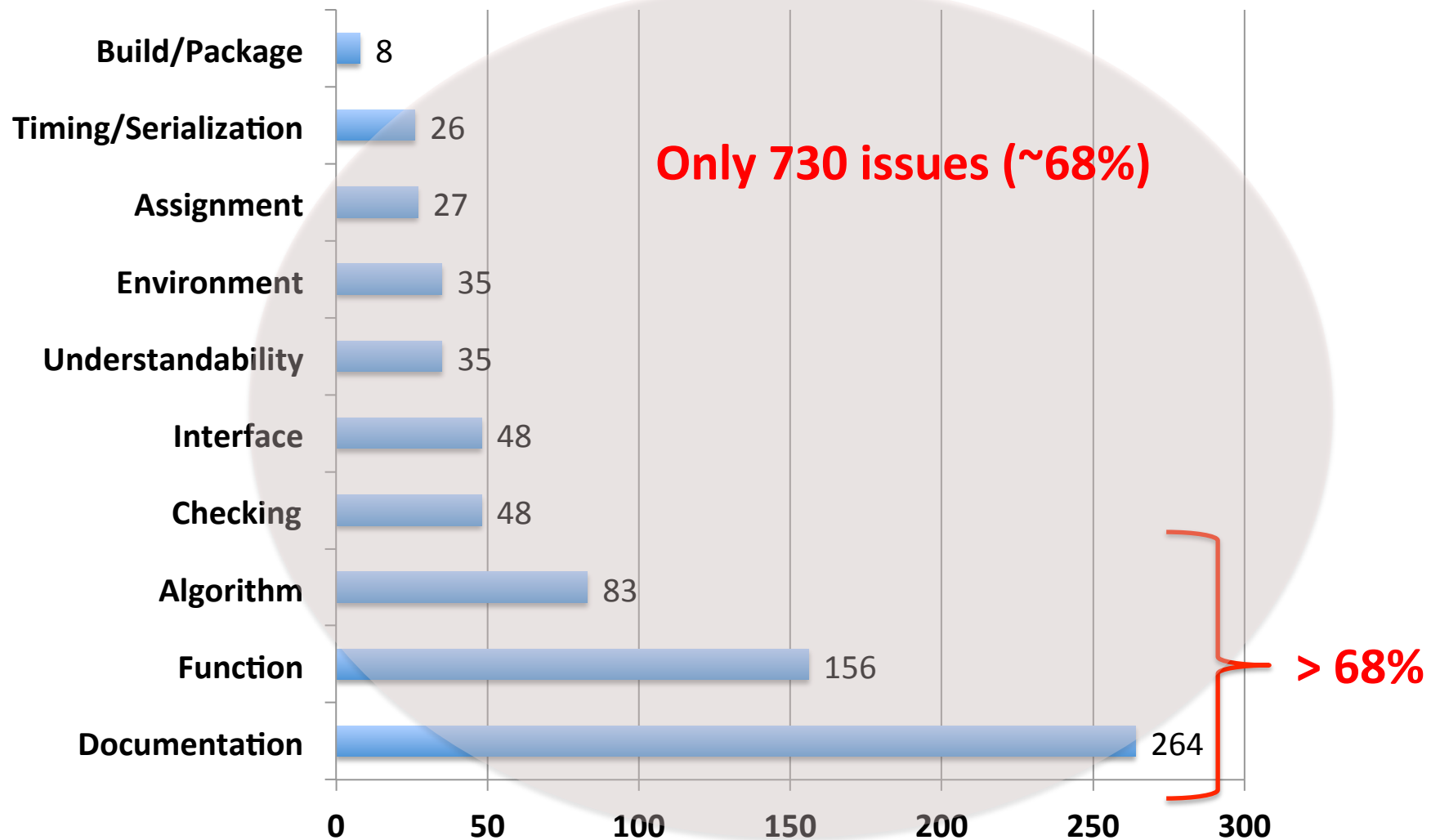


ORIGINAL ISVV CLASSIFICATION

Problem Type	# Issues	%
External Consistency	313	29%
Completeness	275	26%
Correctness	213	20%
Internal Consistency	132	12%
Technical Feasibility	3	<1%
Readability & Maintainability	84	8%
Superfluous	14	1%
Improvement	34	3%
Accuracy	2	<1%
Total	1070	100%

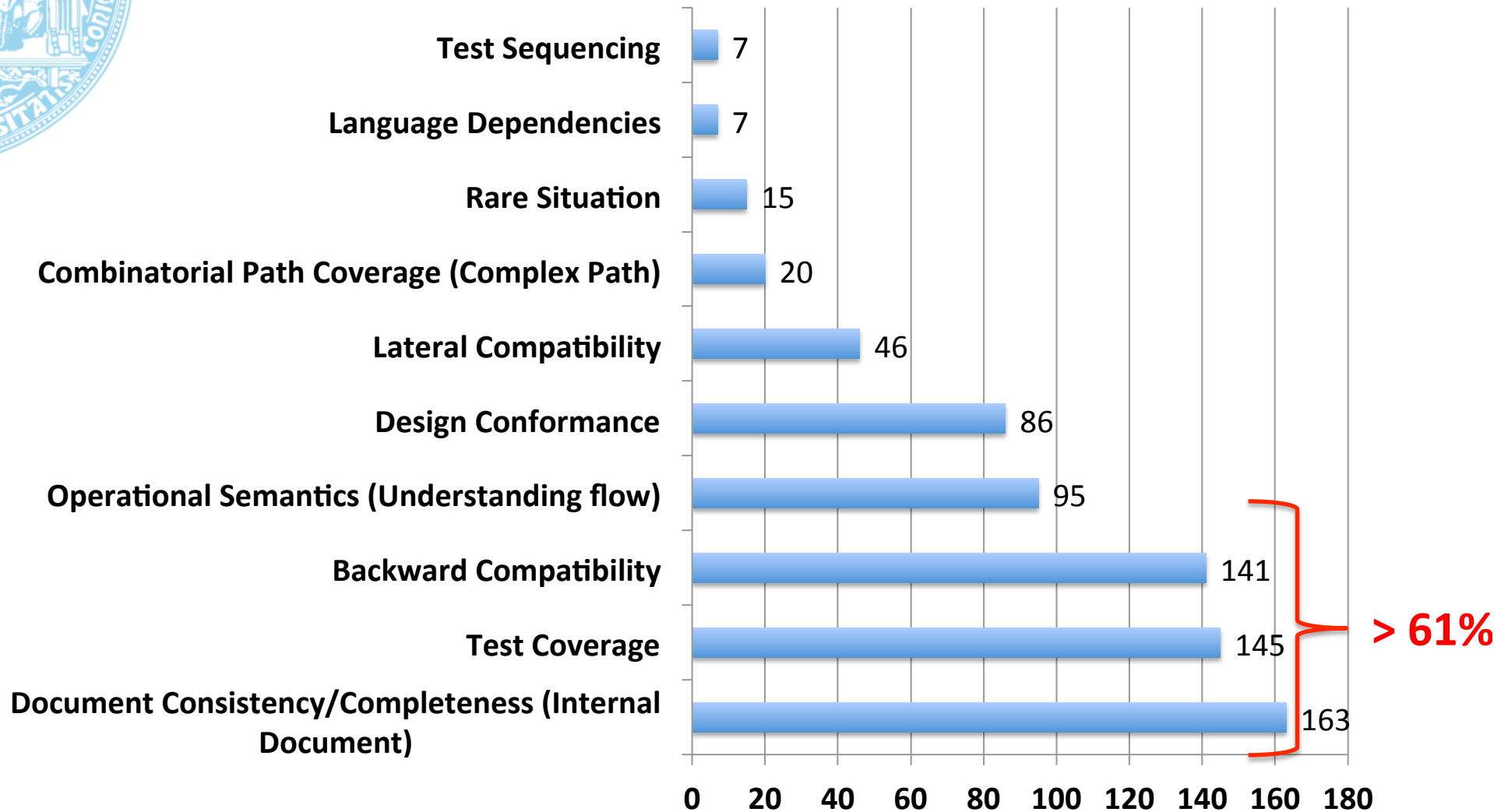


ANALYSIS USING ODC (*TYPE*)



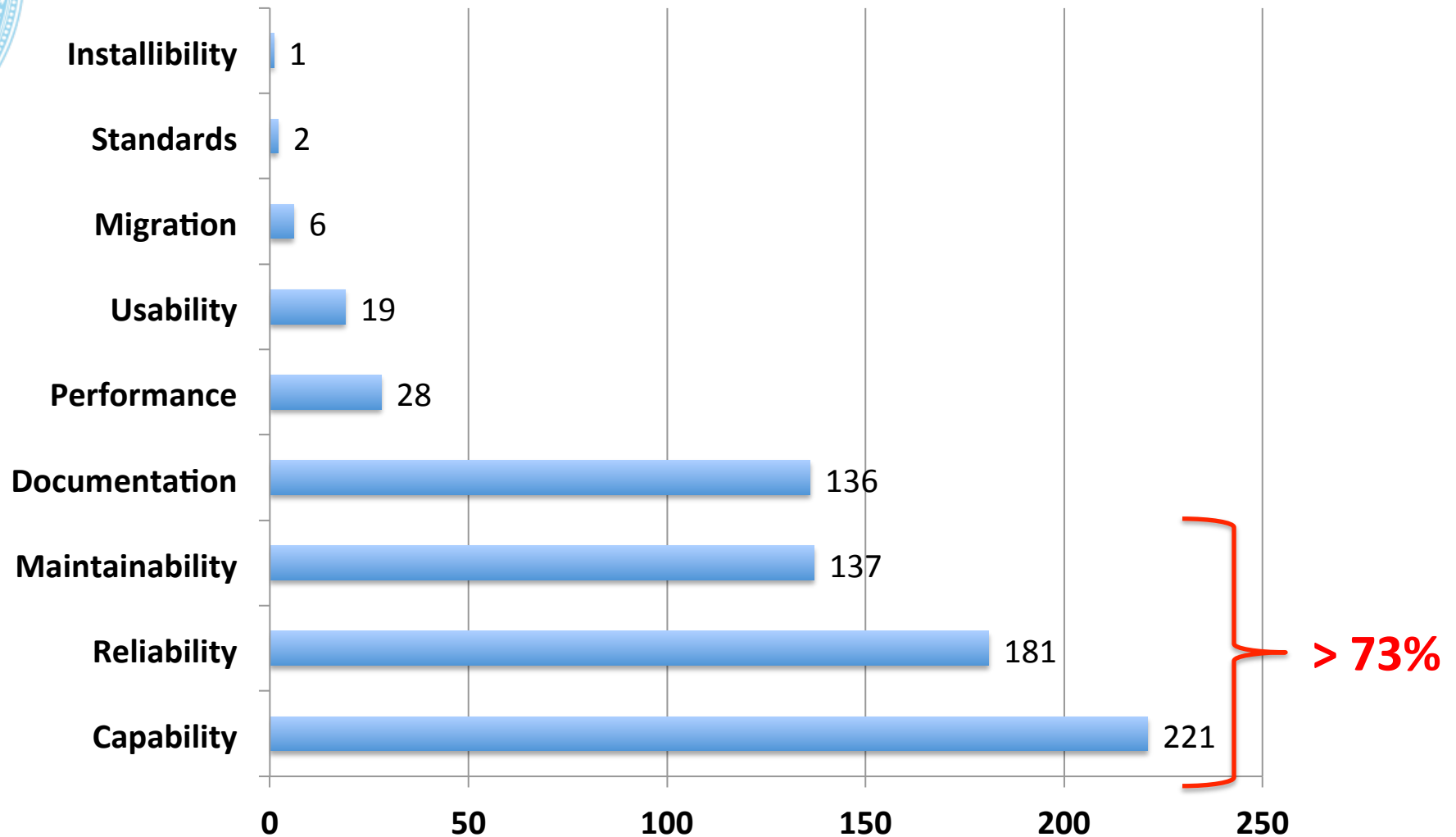


ANALYSIS USING ODC (*TRIGGER*)





ANALYSIS USING ODC (*IMPACT*)





ANALYSIS ACROSS PHASES

	Requirements Verification	Design Verification	Code Verification	Test Verification	Ground Monitoring	Total %
Requirements	162	6	10	20	1	199 18.6%
Design	0	106	77	0	6	189 17.6%
Implementation	0	0	289	8	0	297 27.7%
Testing (UT/IT + System Tests)	0	0	2	370	9	381 35.6%
Operation	0	0	0	0	4	4 0.37%
Total	162	112	378	398	20	1070
%	15.1%	10.4%	35.3%	37.2%	1.8%	100%



RECOMMENDATIONS (1)

Reinforced importance of documentation quality measures

- Namely documentation reviews
- Need for improved requirements engineering, requirements analysis techniques or tools and requirements testing
- Promotion of traceability analysis between every phase of the engineering process
 - If possible automation of these *traceabilities*...



RECOMMENDATIONS (2)

- Test improvements, test coverage improvement, and specific validation plan guidelines shall be proposed
 - Help engineering in defining better and more complete tests
 - Focus on requirements coverage, both functional and non-functional
- Reliability and Dependability analysis shall be performed in a more efficient way:
 - Integrated at all lifecycle phases
 - Start earlier
 - Become more extensive
 - Automated and
 - Promote traceability and historical results follow-up

CONCLUSIONS

■ **Goal 1:** Relevance of ISVV

- Confirmed!
- Many relevant issues captured by ISVV in different phases

■ **Goal 2:** Real issues in aerospace critical systems

- Large number of issues identified, some during operation
- Standards help, but not completely!

■ **Goal 3:** Applicability of ODC

- Needs to be extended

■ Other safety critical industries may also learn from this

...



QUESTIONS?

Marco Vieira

Department of Informatics Engineering
University of Coimbra

mvieira@dei.uc.pt

<http://eden.dei.uc.pt/~mvieira>

