Dependable Technologies For Critical Systems

Software Role in Future Space Missions

A Critical Software View

Paulo Guedes

Business Development Manager

Agenda

1962 – Mariner I Space Probe

"The most expensive hyphen in history“ – Arthur C. Clarke

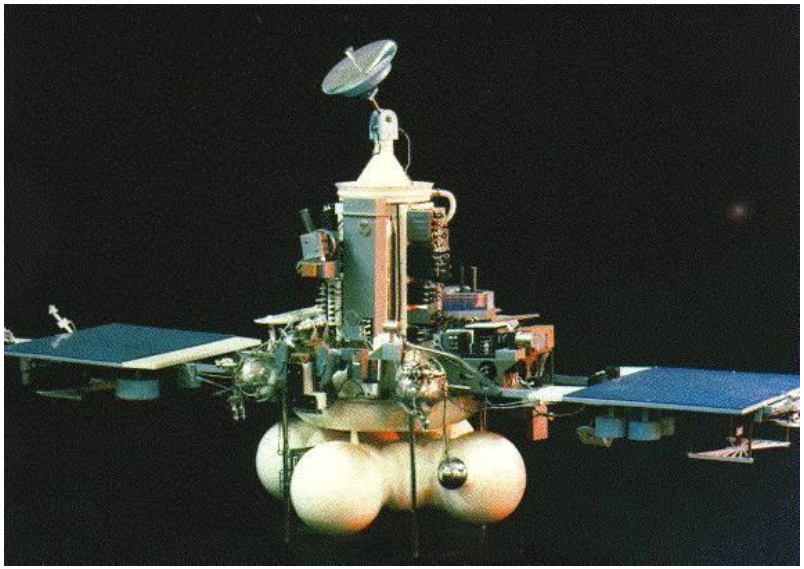
Top 10 History’s Worst Software Bugs - Wired Magazine

- A bug in the flight software for the Mariner 1 causes the rocket to divert from its intended path on launch
- A formula written on paper in pencil was improperly transcribed into computer code, causing the computer to miscalculate the rocket's trajectory
- Mission control destroys the rocket over the Atlantic Ocean

1988 – Phobos 1

- Loss of communication and failure to regain contact
- De-activation of attitude thursters
- Error in the uploaded software – routine coded in PROMs

"Why would a spacecraft have instructions that turn off the attitude control, normally a fatal operation?"

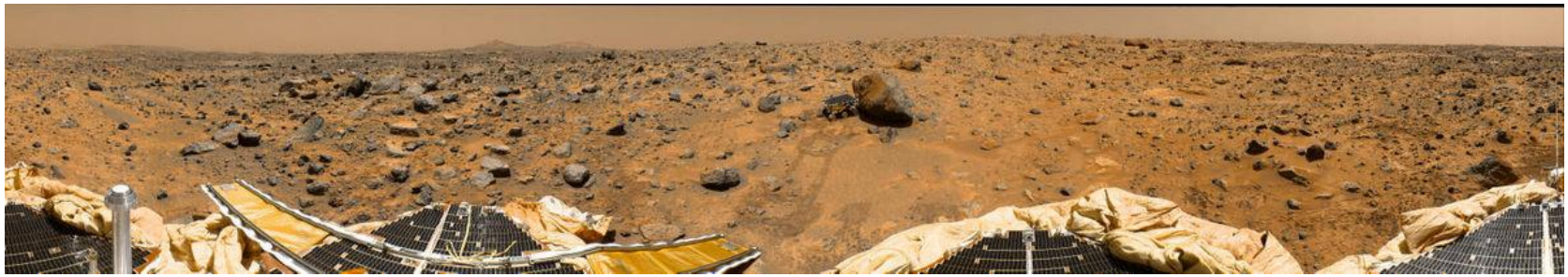


1996 - Ariane 501

- Inappropriate reuse of a component in Ariane 4's inertial reference frame software
- Lack of sufficient documentation describing the operating constraints of the software
- Unprotected conversion from a 64-bit floating point to a 16-bit signed integer value overflowed
- Top 10 History's Worst Software Bugs *

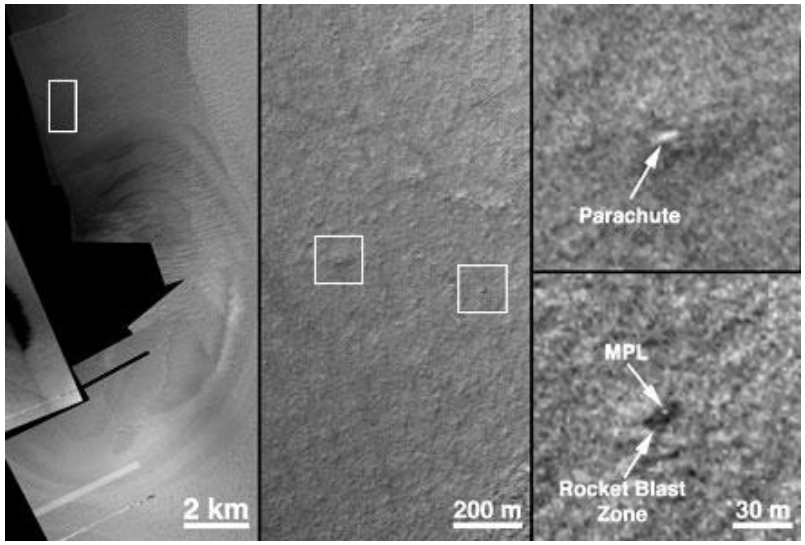
* Wired Magazine

1997 - Mars Pathfinder



- Loss of science data caused by infrequent, mysterious, unexplained system resets experienced by the Rover
- Priority inversion bug in simultaneously executing processes
- Anomaly impossible to detect with black box testing

1999 - Mars Polar Lander



Programme "was under funded by at least 30%."

"The software—intended to ignore touchdown indications prior to the enabling of the touchdown sensing logic—was not properly implemented [...]"

- Landed at 22 meters per second
- Shutdown of descent engines 40 meters above the surface
- Software identified vibrations as surface touchdown
- Altough known, software did not account for it

2006 – Mars Global Surveyor

"The loss of the spacecraft was the result of a series of events linked to a computer error made five months before the likely battery failure“
"We are making an end-to-end review of all our missions to be sure that we apply the lessons learned from Mars Global Surveyor to all our ongoing missions"

- Loss of contact after command do adjust power panels
- Overheating batteries led to complete power deplition
- Failure to relay communications
- Flaw in software parameter update

Critical

Dependable Technologies For Critical Systems

Lessons Learnt

Lessons…

- Software errors are latent design errors
- Complexity of software
- Performance optimizations
- Reuse qualified software is not necessarly safe
- The human coding component still has a huge wheight in the process
- Budget and schedule constraints are enemies of “perfection”

Learnt?

Critical

Dependable Technologies For Critical Systems

Future Space Missions

Space in the 21st Century

Human Exploration

Year	Mission
2020	Landing Moon
2030	Landing NEO
2035	Permanent Lunar Base
2040	Landing Mars
2040	SSTO Launcher
2070	Landing Europa (Jupiter)
2090	Permanent Martoan Base
2090	Landing Enceladus (Saturn)

Human Exploration

- Longer missions
- Science-Astronaut roles
- Robotic support
- Independant initiative

Mix-initiative Environments

Human-Centered Computing

- More potential execution paths dependant on continuous stream of human inputs
- Understandable and predictable
- Current Development and V&V methods are inadequate

Autonomous Spacecraft and Rovers

- Adaptable (smarter) and self-reliant (independent) in harsh and unpredictable environments

- Robust and autonomous software
- Highly responsive
- Complex navigation skills

- More “execution paths”
- Increasing “behavior” possibilities

- Autonomous onboard science capability
- Communication requirements

- Increasing processing power and capability
- Complexity increase

Influencing (and Risk) Factors

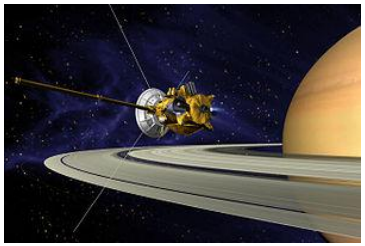
- Cost-effectiveness
  - Increased complexity
  - Tightly coupled
- Human-Centered Computing
  - Paradigm shift
- Software already poses considerable risks
  - Reluctance in adoption
  - Hurdle in deploying new technologies
  - Need for V&V in specific contexts

Dependable Technologies For Critical Systems

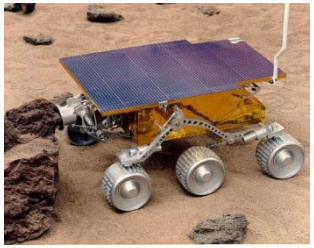
The Future of Software Role

Exponential Growth

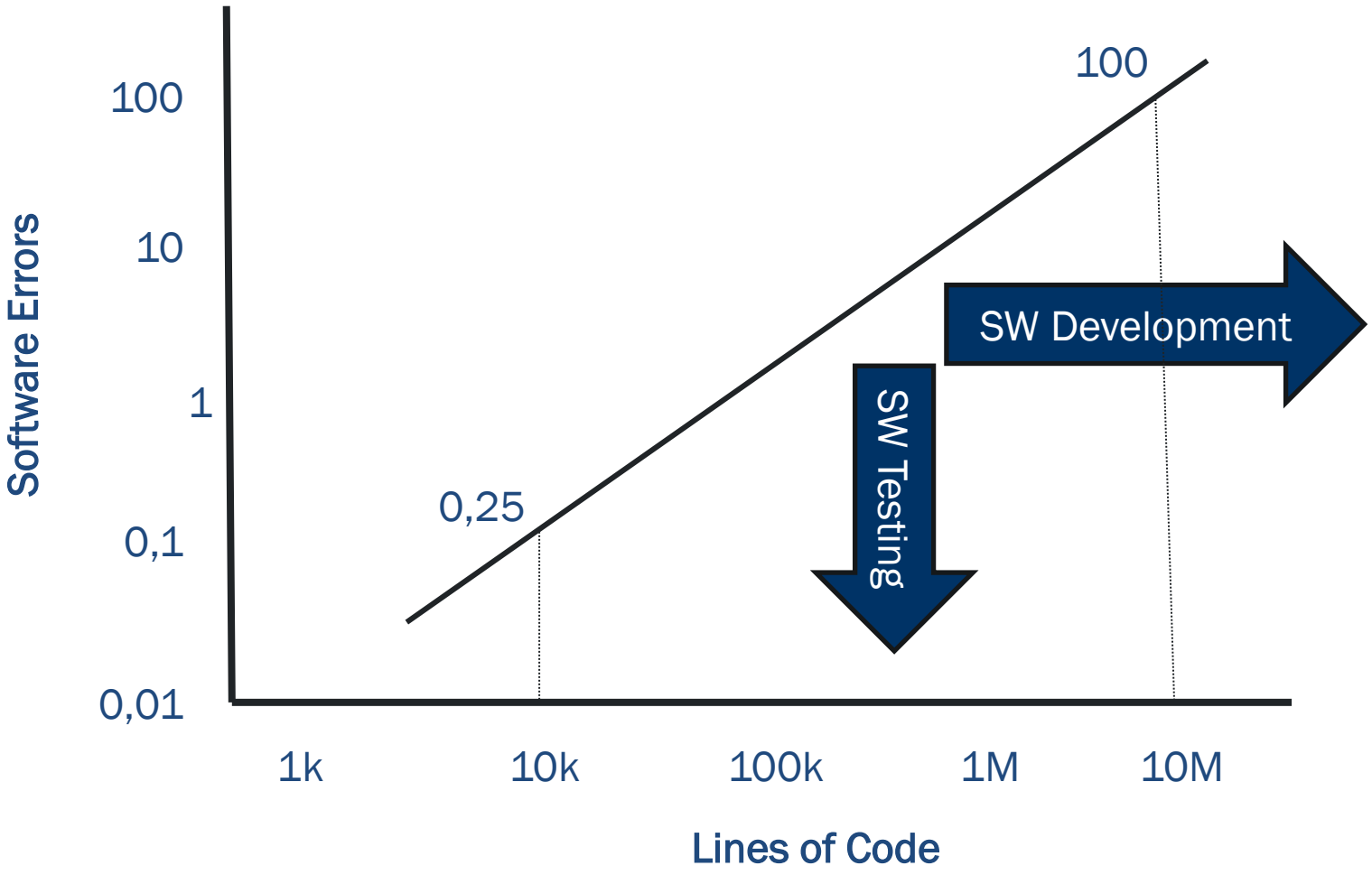
Mission	Launch Year	Thousands SLOC
Voyager	1977	3
Galileo	1989	8
Cassini	1997	32
Mars Pathfinder	1997	160
Space Shuttle	2000	430
ISS	2000	1700





Objective



Dependable Technologies For Critical Systems

Software Development

Improve Cost and Schedule

- Software Contruction Technology
  - Autocoders
  - Rapid Development Environments
- Approach breaks down for Mission-Critical or Safety-Critical Software
  - Certification costs dominate development costs
  - Certification needs to be done at a higher level and then translated to lower level

Improve Cost and Schedule

- Building Block (Software)
  - Clear; Performant; Self-contained; Quality; Applicability; Repeatability; Relevant; Reuse; COTS
- Based on well-defined Specification & Interfaces based on an agreed Reference Architectures
  - Streamlined development
  - Stimulate development
  - Standardize avionics

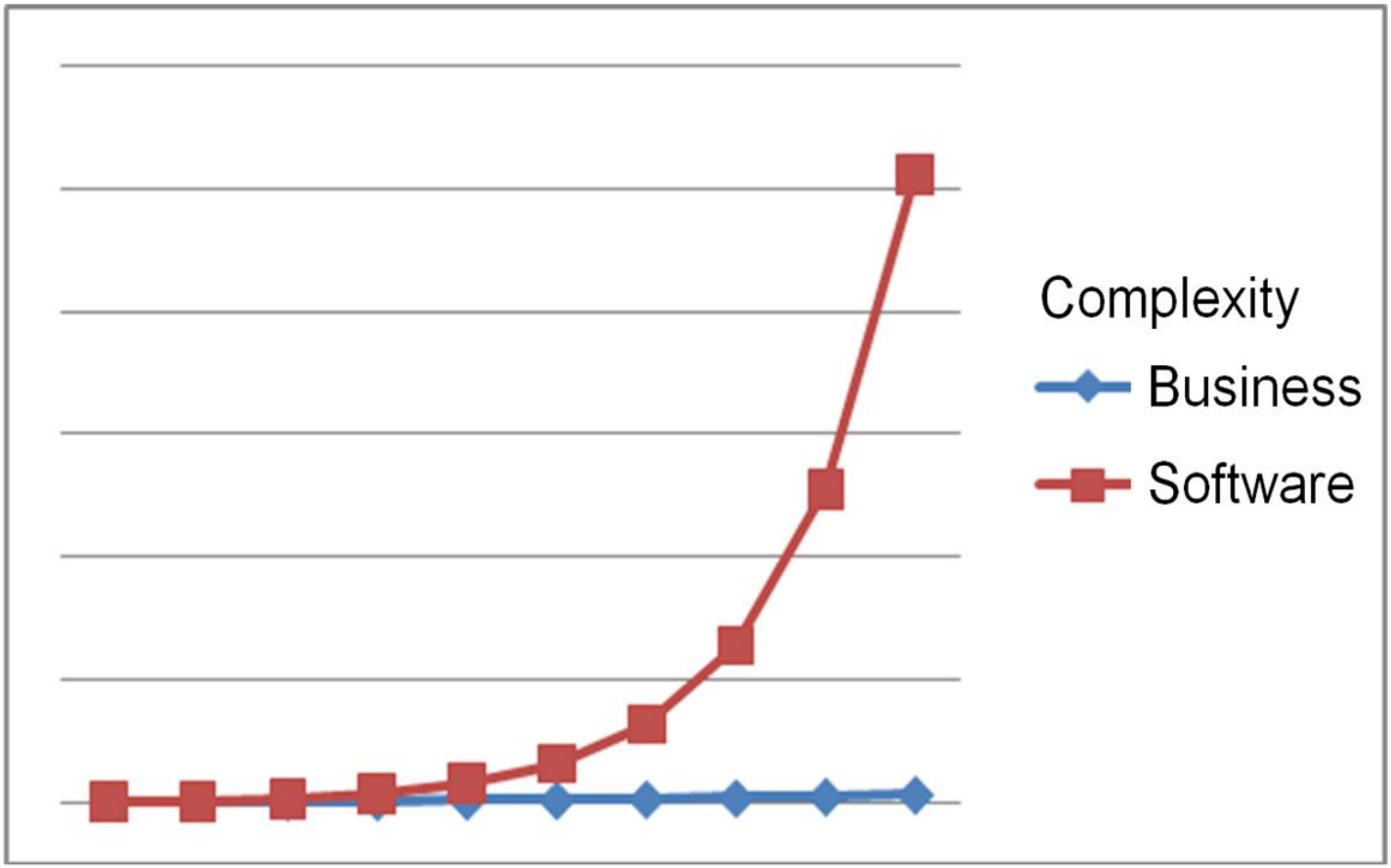
Increase Reliability

- Increase Reliability as Complexity Increases
  - Development for Certification
  - Technology that ensures reliability and addresses certification issues
- Changing Software Contruction Technology
- Changing Software Development Processes and Approaches

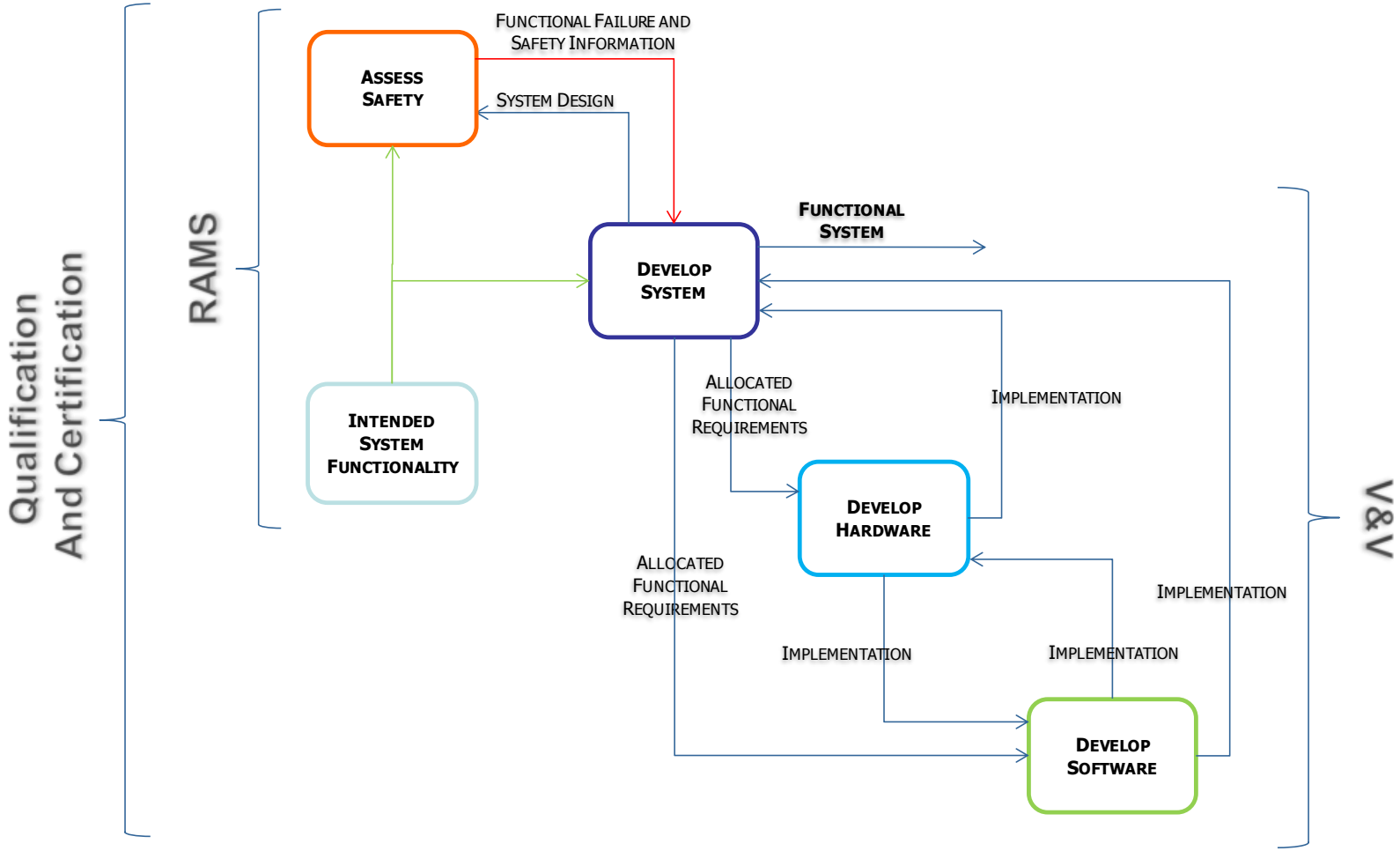
Dependable Technologies For Critical Systems

Software Testing

Software Testing



Engineering Techniques

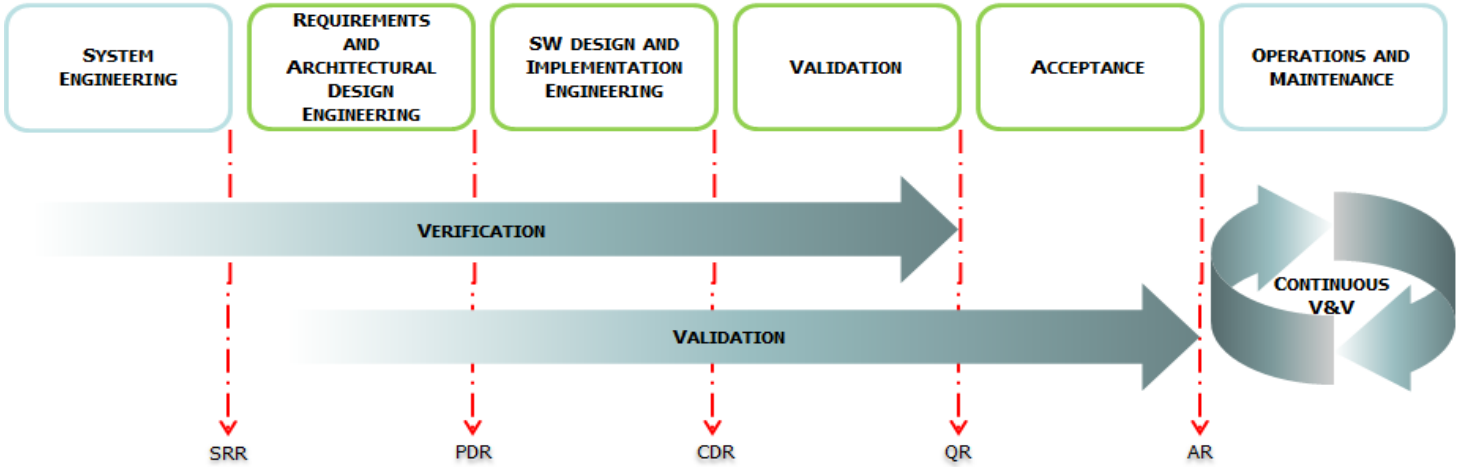


RAMS

- Set of techniques and analyses to assess the safety and dependability of a system
- When applied early enough in the development life cycle, can have a major impact on decisions regarding the design of sub-systems contributing to a more dependable and safe system that can be designed and developed at a lower cost
- Great engineering support during requirements and architecture phases
  - Input for requirements completeness and coherence

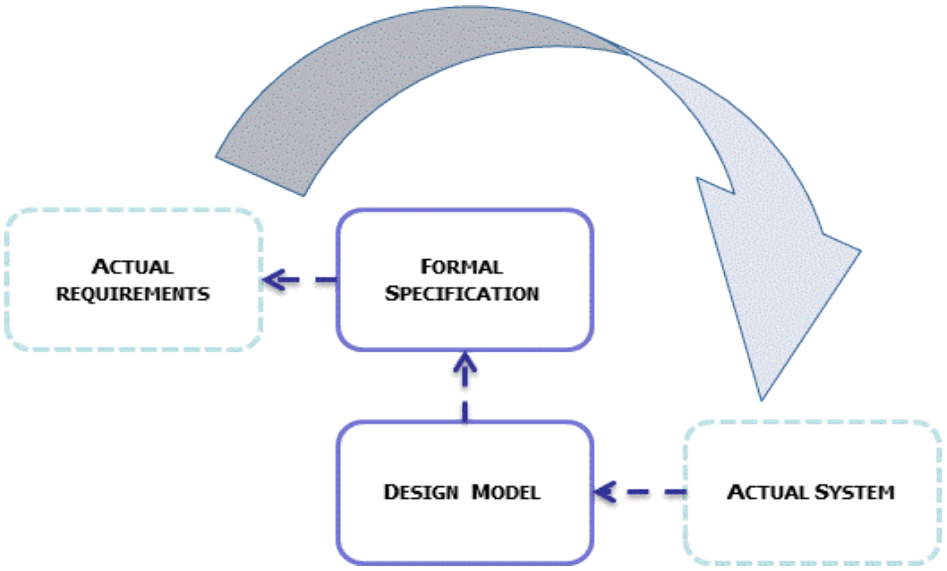
Verification & Validation

- Involve the final user, system, hardware and software development, and are present from the planning of a system to the acceptance of the functional system against the intended system functionality
- Guarantee system free of faults and performs according to the respective specifications
- Applicable to all levels / early error detection



Formal Methods

- The use of mathematical techniques to ensure that a design conforms to some precisely express notion of functional correctness



- Requirements and early system prototypes can all be represented in rigorous notations which are amenable to automatic verification techniques/tools
- The added cost is compensated by a much more powerful verification

Dependable Technologies For Critical Systems

About Us

CORPORATE PRESENTATION

CRITICAL SOFTWARE AT A GLANCE

- *Spin-off* of the University of Coimbra, July 1998
- Military and Civil Markets with customers around the globe
- Offices in Europe, US, South America and Africa with more than 450 engineers
- Fast growth achieving USD 26M annual turnover in 2009

DEPENDABLE SOLUTIONS FOR BUSINESS AND SAFETY CRITICAL APPLICATIONS

CORPORATE PRESENTATION

OFFICE LOCATIONS

Coimbra, Portugal

Lisboa, Portugal

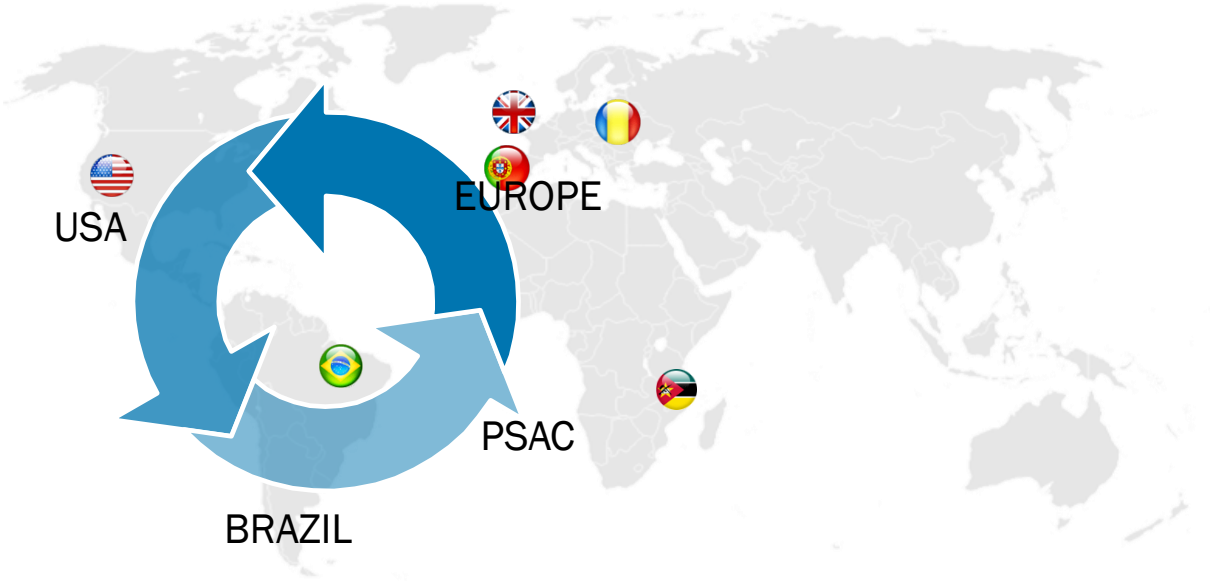
Porto, Portugal

Southampton, UK

Yeovil, UK

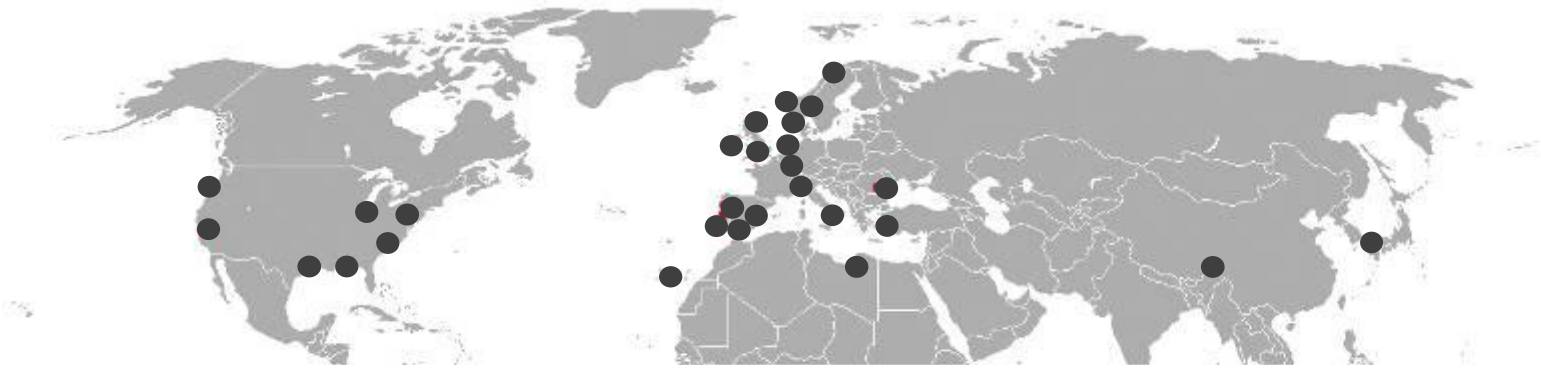
San Jose, CA, USA

Sao Paulo, Brazil



CORPORATE PRESENTATION

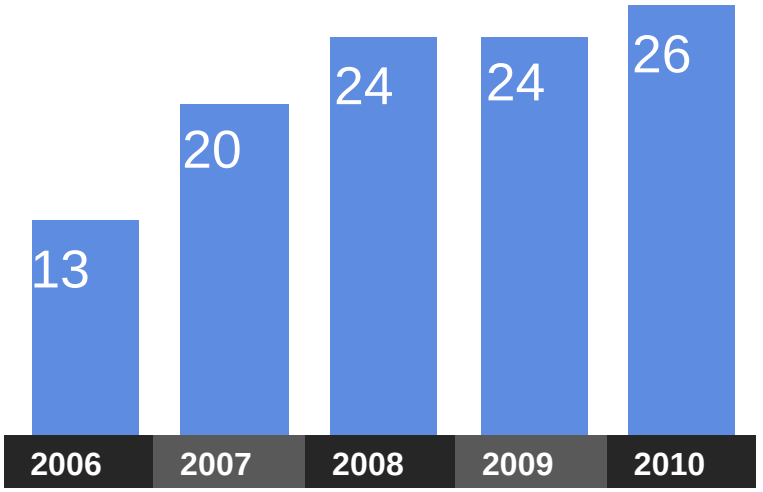
CUSTOMERS AND GEOGRAPHICAL MARKETS



CORPORATE PRESENTATION

FINANCIAL FIGURES

- High-growth profile (organic)
  - –26M in 2010
- Good capacity to generate wealth
  - –EBITDA: between 7% and 21% from year one
  - –Re-investment of all generated wealth
- Strong investment in R&D
  - –10% of *turnover*



TURNOVER IN MILLION USD

CORPORATE PRESENTATION

THE COMPANY'S STRATEGIC PILLARS

CORPORATE PRESENTATION

MARKETS

Critical

Dependable Technologies For Critical Systems

Space

Space Segment and Launchers, Ground Segment, User Segment

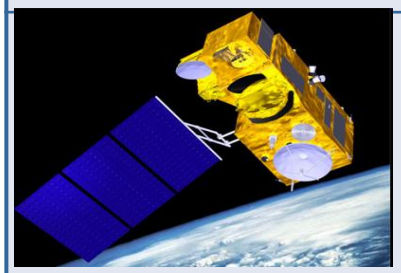
SPACE SEGMENT AND LAUNCHERS

Supplier of software solutions, certifiable services and products for subsystems and interfaces since 1998.

- Safety Critical development of software solutions (real time and embedded, satellite on-board software), real-time systems (specification, design and development, distributed architectures, IMA and data distribution services) and advanced engineering (parallel computing, control engineering and programmable logic);
- Safety Critical Validation: system/software V&V and RAMS, safety critical assessment (on-board and airborne systems); software certification (ARP4754/ARP4761 for airborne and ECSS Q-40 and NASA STD-8719.13 for on-board systems) and software certification support (DO-178B);
- Critical track record includes work with the four main space agencies: ESA, NASA, JAXA, CASC.

SPACE SEGMENT AND LAUNCHERS

ESA SENTINEL MISSIONS

	**Sentinel-1** C-Band SAR payload following a Sun-Synchronous orbit with a 12 days repeat cycle. **Critical Software is responsible by the ISVV.**
	**Sentinel-2** Multispectral instrument spanning from visible to near-infrared; follows a Sun-Synchronous orbit with 5 days revisit time. **Critical Software is responsible by the development of the on-board Central Software (AOCS, MSI and THC Subsystems)**
	**Sentinel-3** Four scientific instruments (OLCI, SLSTR, SRAL and MWR) following a Sun-Synchronous orbit with a 27 days repeat cycle. **Critical Software is responsible by the development of the on-board Central Software (MAS and parts of the SMS)**

GROUND SEGMENT

Supplier of software solutions for mission control, modelling, simulation and control and intelligence (C2I).

- Mission Control Systems (SCOS-2000 Monitoring & Control System);
- Mission Planning Systems;
- Payload Data Processing;
- Simulation systems, particularly Operational Simulators and Validation Facilities, to support the validation of both Spacecraft Instruments and subsystems as well as Ground Control Systems
- Critical track record includes work with ESA and main European primes in the Ground Segment Domain.

GROUND SEGMENT

TECHNOLOGY HARMONISATION – REFA GS SW

Challenge

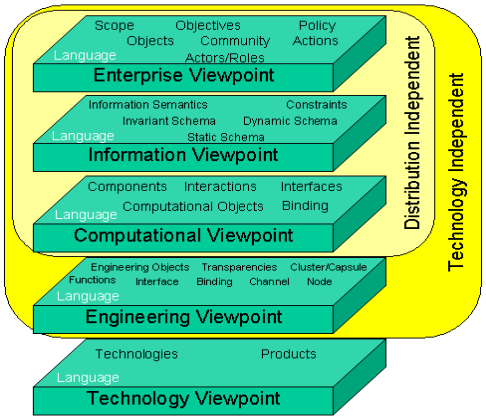
- Reduce diversity of products used in the ground segment and improve interoperability

Solution

- Specify standard functions, interfaces and services using a methodology which combines RM-ODP, SOA and MDA
- Usage of Platform Independent Models (PIM) and Platform Specific Models (PSM)

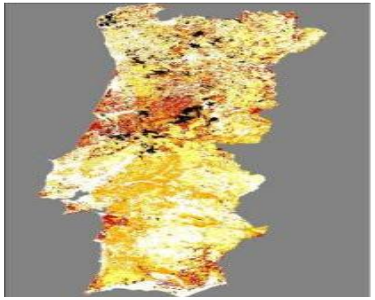
Benefit

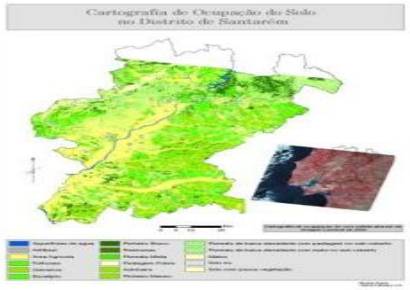
- High Level Requirements for the Ground Systems Software.
- Reference Architecture for Ground Segment Systems encompassing Information, Service and Interface Model
- Standard ICDs which can be reused in a wide variety of ESA Missions



USER SEGMENT

Supplier of Earth Observation solution and Downstream and User Segment services.





- Earth Observation Emergency Services: fire monitoring, burned areas, lanslides and flooding mapping;
- Earth Observation Land Services: land cover and land use, desertification monitoring, forestry management, spatial planning (forecast and urban land use planning); water monitoring (water balance, flow rates and depths of rivers and lakes, soil moisture level);
- Critical track record includes work with the Portuguese Ministry of the Interior, pulp and paper producers, ESA, the Portuguese Navy, the European Community and the World Bank.

USER SEGMENT

RIO DE JANEIRO LANDSLIDE PREVENTION

Challenge

- Demonstrate the usage of VHR imagery in the identification and classification of housing built in order to:
  - Improve Urban development (identify vacant, under-utilized or industrial areas - along new transport investments - for housing development;
  - Define flooding scenarios on low-lying areas;
  - Support the identification of housing built on areas at risk of floods (low-lying areas) or landslides (steep hills).
- Integrated in EO World initiative for the State of Rio de Janeiro

Solution

- Provision of high resolution DEM and Slope maps
- Production of VHR Land Use with hierarchical nomenclature for multi-scale analysis and applications
- Floods Risk Scenarios based on Land Use, DEM and historical meteorological data
- Land Slide Risk areas

Benefit

- Actuate preventively to discourage informal settlement on risk areas
- Identification of land for further urban development

WORLD BANK

esa

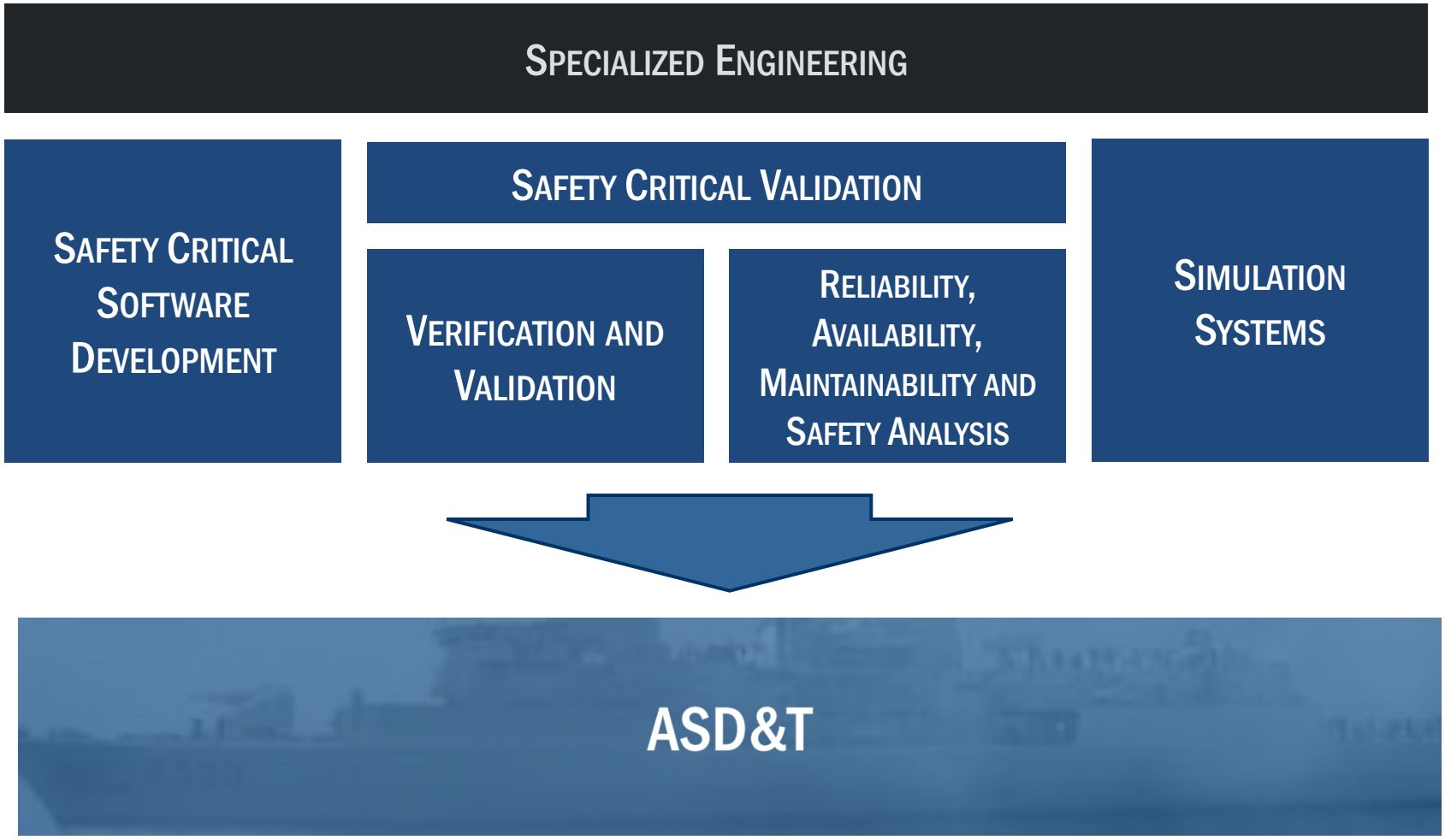
eoworld
Earth Observation for Development

Dependable Technologies For Critical Systems

Specialized Engineering

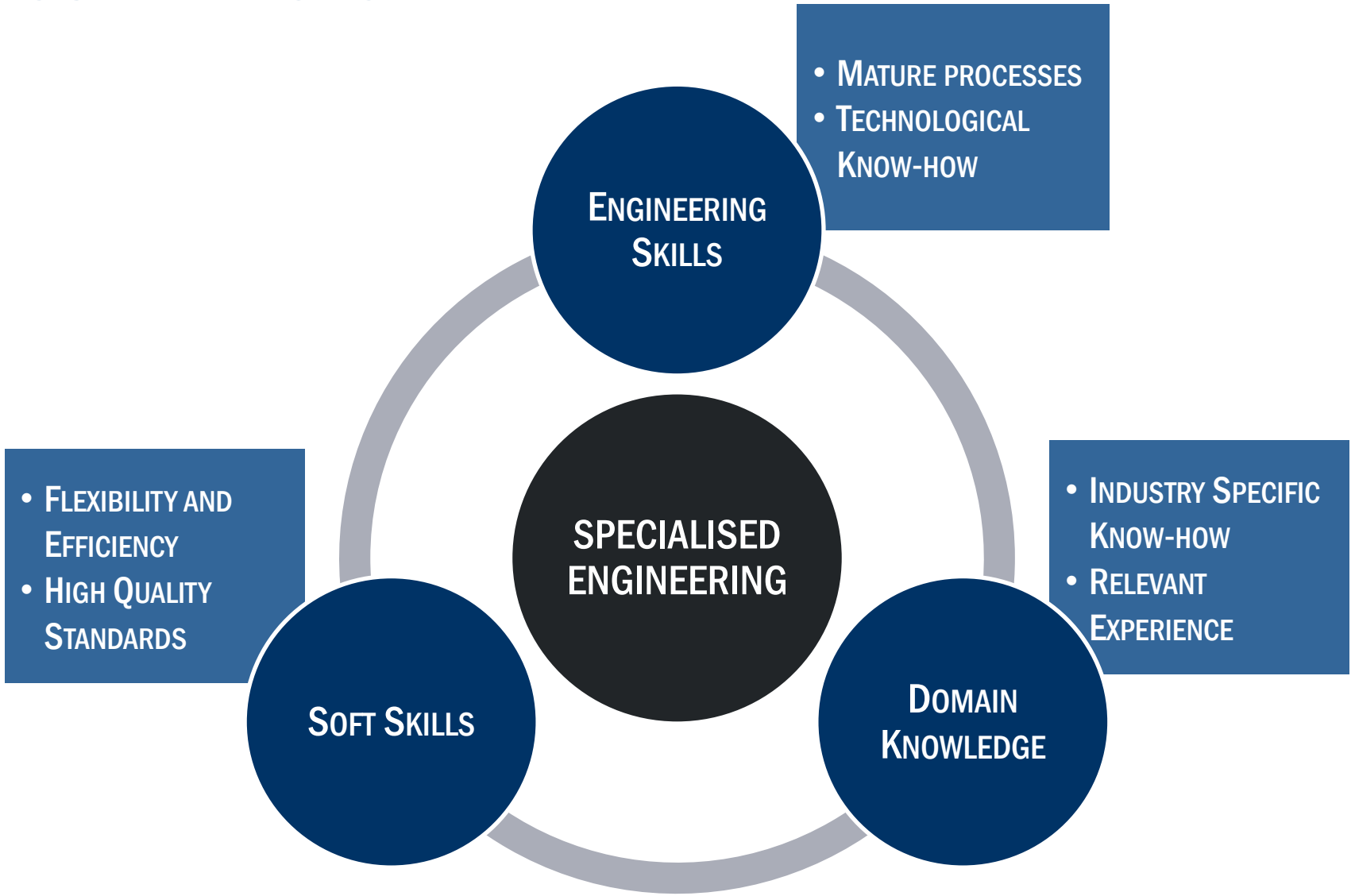
SPECIALISED ENGINEERING

OVERVIEW



SPECIALISED ENGINEERING SERVICES

OUR APPROACH



Dependable Technologies For Critical Systems

Paulo Guedes – Business Development Manager

pguedes@criticalsoftware.com

Rua Eng. Frederico Ulrich, nº 2650
4470-605 Moreira da Maia
Portugal

www.criticalsoftware.com