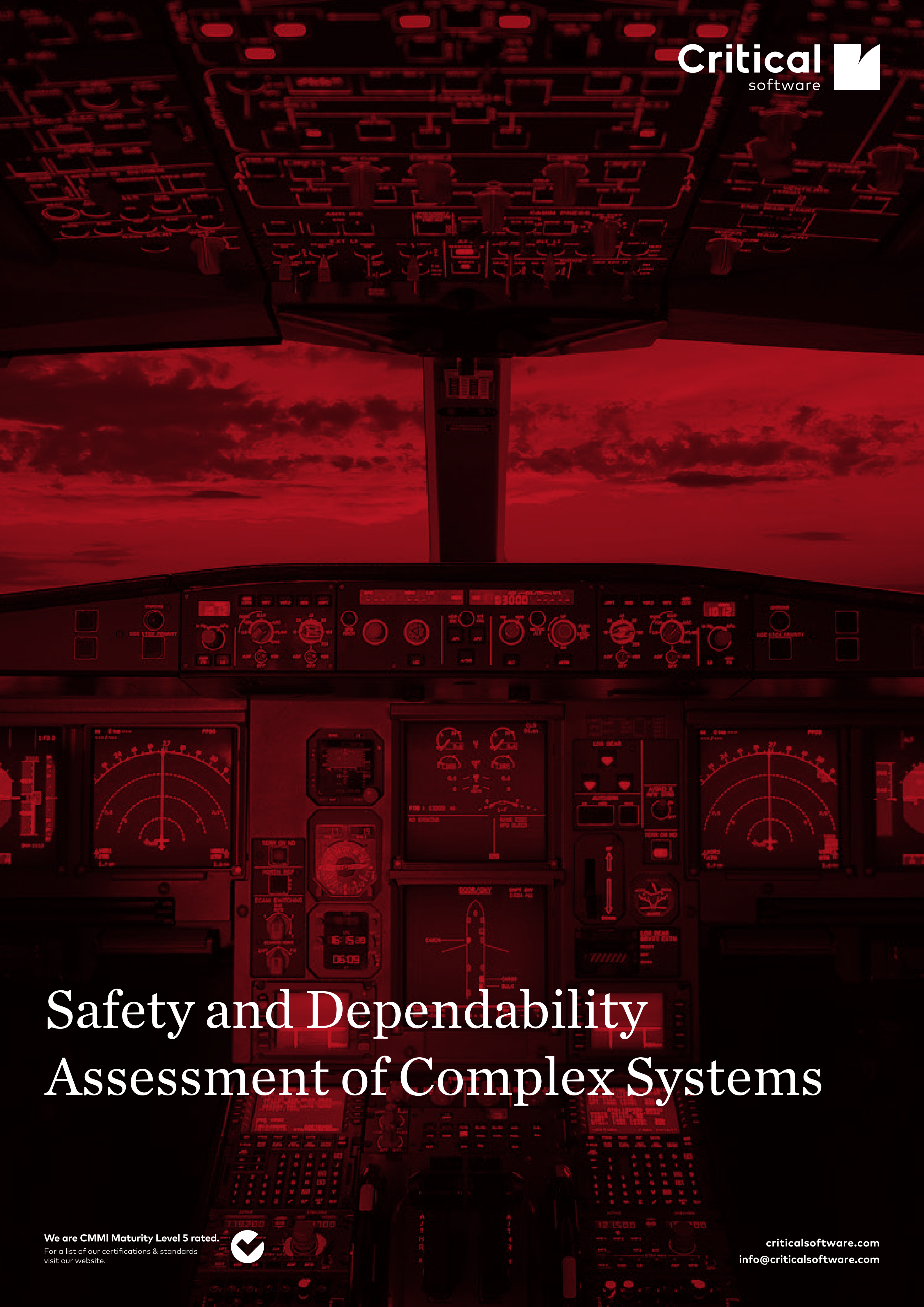


Critical software

Safety and Dependability Assessment of Complex Systems

We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards visit our website.

criticalsoftware.com
info@criticalsoftware.com

Safety and Dependability
Assessment of Complex Systems

RAMS (Reliability, Availability, Maintainability and Safety) supports certification by providing a set of techniques and analysis to assess systems' safety and dependability. It has a major impact on design decisions and contributes to more dependable and safer systems, designed and developed at lower cost.

Multiple iterations are performed at different phases of development, to ensure full coverage of functionality.

Critical Software has fifteen years' experience in providing RAMS services to support product certification in several markets, including aeronautics, meeting their respective standards: DO-178B/C, RIAC 217Plus and FMD-97.

Critical Software can apply RAMS analysis to systems under development and to systems already in production that need upgrading or re-qualification.

DEPENDABILITY ANALYSIS

Critical Software is focused on reliability and its influencing factors.

Dependability is treated as an aggregation of:

- **Reliability**: to ensure the ability of a system or component to perform the required functions in defined conditions for a specific period of time.
- **Availability**: to assess the percentage of time within a given lifespan (usually the system's functional life) in which the system is functional.
- **Maintainability** (serviceability and repairability): to support the definition of the characteristics of design and installation that determine the probability that failed equipment, machines or systems can be restored back to operation within a given time and cost.

Software dependability is characterised by qualitative rather than quantitative analysis. Reliability is ensured by the identification of failure modes, failure propagation paths and the implementation of failure barriers, as well as the implementation of adequate software development and validation methods.

Hardware dependability is quantitatively-oriented, and is achieved by characterising all low-level components, modelling the hardware architecture and analysing failure modes and failure propagation paths. All relevant electronics and mechanical components are assessed according to industry-applicable standards.

FUNCTIONAL SAFETY ASSESSMENT

Critical Software's safety assessment methods ensure that the accepted level of risk is not exceeded with respect to the factors being evaluated.

Safety assessment is always integrated within a broader safety programme that covers the execution of a set of activities that identify the risks and causes of system failures. These could, in a single or chained set of events, lead to system breakdown and consequently to a big problem.

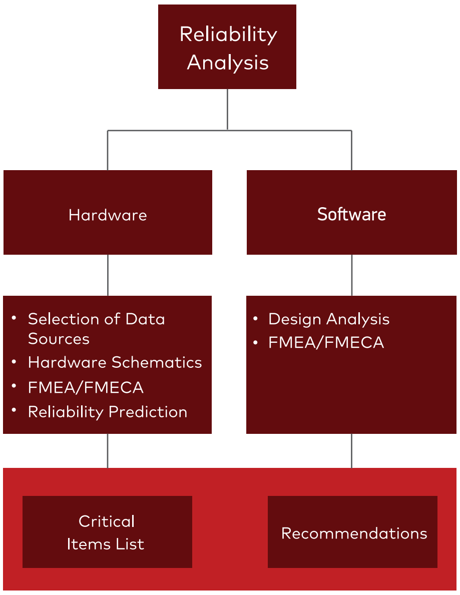
The safety assessment determines the system components' criticality levels and affects both the way the system is developed (lifecycle processes) and the way it is validated.

The results of the safety assessments performed by Critical Software often generate a set of safety requirements that end up by being incorporated into the system specification.

GRAP – CRITICAL SOFTWARE'S OWN METHODOLOGY

Our RAMS experience comes from working in different industry domains. This supported our development of proprietary methods common to different sectors.

GRAP (Generic Reliability Analysis Process) is a coherent, consistent process that guarantees efficient and cost-effective practices for performing system reliability analysis. GRAP is compliant with the applicable market standards in the following industries, including aeronautics.


Reliability Analysis

Hardware

- Selection of Data Sources
- Hardware Schematics
- FMEA/FMECA
- Reliability Prediction

Software

- Design Analysis
- FMEA/FMECA

Critical Items List

Recommendations

ASSESSMENT TECHNIQUES

Critical Software uses several techniques to assess system safety, including:

- Functional Analysis
- Count/Stress Part Analysis
- RAM Prediction, including
  - MTBF, MTTR and Availability prediction
  - Level of Repair Analysis
  - Maintainability Plans
- FMECA
- FTA
- Reliability Block Diagrams modelling (RBD)
- CCA
- HA
- Hardware Software interaction Analysis (HSIA)

BENEFITS

The RAMS methodologies performed by Critical Software:

- Reveal system failures caused by hardware/software or usage errors.
- Mitigate feared system events in early development stages.
- Employ systematic use of techniques, such as FMEA at the software/hardware level, contributing to an overall increase of confidence at system level.
- Focus on the most critical systems, sub-systems and components (hardware and software) offering decisions and justifications for certification purposes.
- Ensure cost-effective activities to address market-specific needs.
- Are performed by highly experienced engineers, with a proactive attitude, providing recommendations and alternative solutions.
- Provide independent assessment, avoiding conflicts of interests at several levels - technical, managerial and financial.
- Help to optimise maintenance plans designed according to system requirements, leading to significant maintenance cost reductions.
- Include techniques performed with the support of state-of-the-art commercial tools, leading to increase efficiency and lower costs.