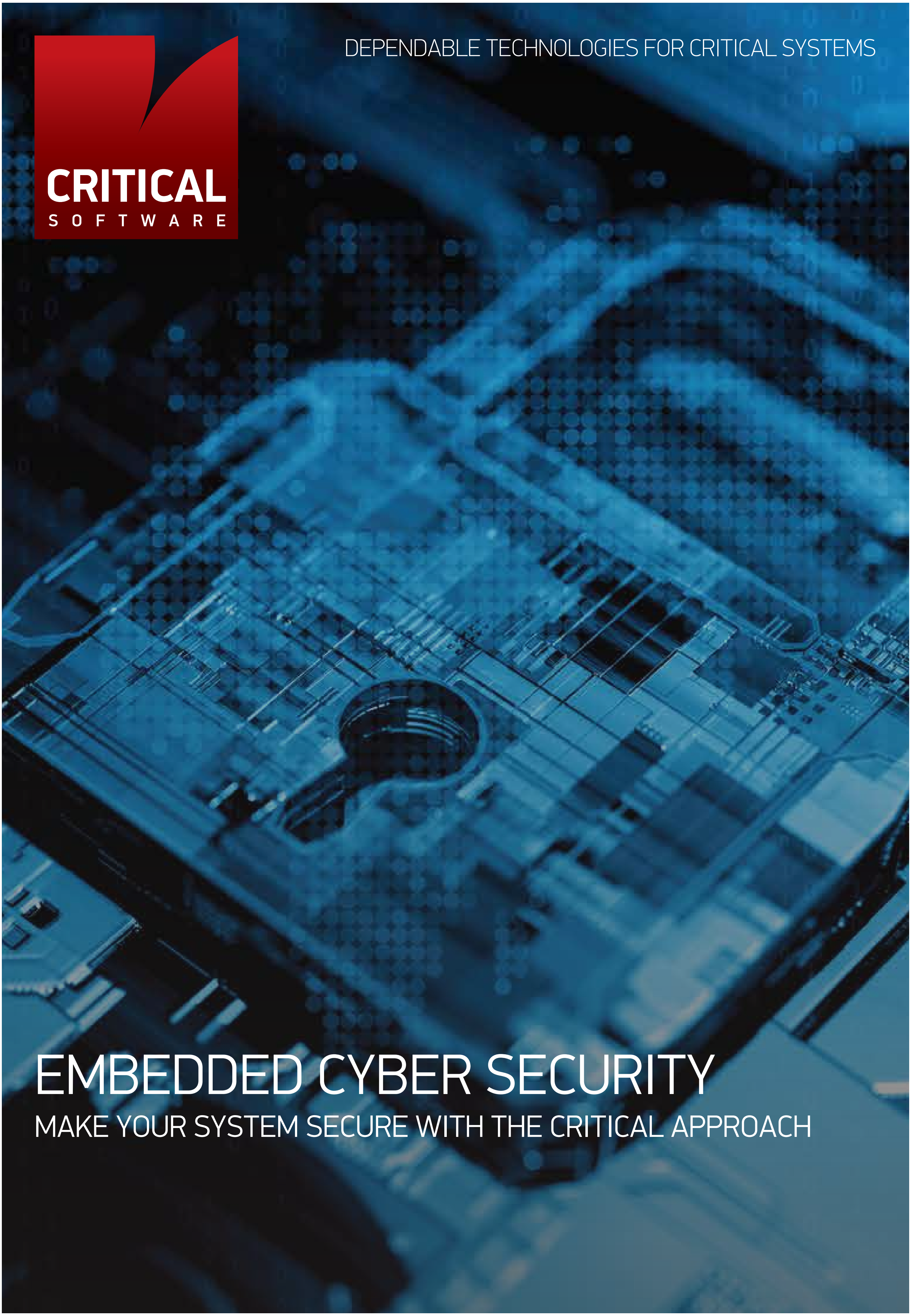
CRITICAL SOFTWARE

DEPENDABLE TECHNOLOGIES FOR CRITICAL SYSTEMS



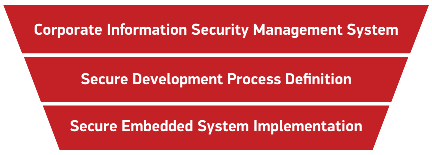
EMBEDDED CYBER SECURITY

MAKE YOUR SYSTEM SECURE WITH THE CRITICAL APPROACH

With potentially vulnerable sectors like aerospace, transport and healthcare adopting more connected embedded systems, maintaining security is increasingly becoming a real problem. The security barriers needed are now much more complex than before, creating a significant challenge for engineering teams.

THE CRITICAL APPROACH

Focusing on the most important aspects of a secure development lifecycle, CRITICAL Software's three-stage approach covers the entire spectrum of embedded cyber security activities, ensuring security policies are enforced across a company.


Corporate Information Security Management System
Secure Development Process Definition
Secure Embedded System Implementation

Based on all or a combination of these three layers, the foundations for the development of secure embedded systems are set.

1. CORPORATE INFORMATION SECURITY MANAGEMENT SYSTEM

Each development of an integrated electronic system or software package is supported by a set of tools, networks and IT systems which are part of a company's day to day operations, holding vital information. During the first stage, we focus on supporting systems and the level of information security in effect.

SCOPE: supporting systems and overall information security

KEY ACTIVITIES: implementation of an Information Security Management System (ISMS)

DELIVERABLES: definition of security roles, security processes and security guidelines

2. SECURE DEVELOPMENT PROCESS DEFINITION

In the second stage, we look at defining and safeguarding the development process. This includes adapting existing development processes to make them more secure; even with an existing system development process in place, enhancement is often necessary to enable production of secure embedded systems.

SCOPE: defining a secure development process

KEY ACTIVITIES:

- Identification of gaps in the existing development process and associated security aspects
- Set up strategy for the development or update the existing process
- Preparation of a security management plan

DELIVERABLES:

- Definition of secure development process
- Security management plan
- Specific development guidelines for secure development of systems

3. SECURE EMBEDDED SYSTEM IMPLEMENTATION

The third and final layer of our approach is dedicated to the implementation of secure embedded systems. Covering all key areas, we provide a set of activities for development teams, helping companies build more secure systems going forward.

SCOPE: implementation phase

KEY ACTIVITIES:

- Secure system development
- Introducing security in legacy systems
- Security threats and vulnerabilities analysis (STECA methodology)
- Independent risk analysis
- Specific security analysis
- Requirements review
- Design review
- Software code review
- Test cases review
- Penetration test specifications and execution

DELIVERABLES:

- Threats and vulnerabilities analysis
- Security requirements
- Security barriers analysis
- Security dossier for compliance with applicable regulations

BENEFITS

- Complete coverage of all embedded cyber security needs
- Flexibility to target even the most vulnerable areas
- Compliance with the most demanding international security guidelines

61%

61% of embedded systems are designed with the expectation that they will connect to the internet.

38%

38% of developers of safety-critical systems are neglecting to follow any relevant safety standards.

29%

29% of embedded systems could cause injury or death were they to fail or be used in an irresponsible way.

EXTRA SUPPORT

Many companies already have a quality management system in place but it's likely that this is simply not enough to combat current security threats and, in almost all cases, this system will need to be enhanced. In such cases, CRITICAL Software offers an additional consultancy service. Our knowledgeable engineers can support and lead the overhaul of internal processes, helping an organisation to shift to a more security-conscious culture. Our service covers all key elements like gap analysis, definition of security processes and day-to-day management going forwards.

WHY CRITICAL SOFTWARE?

We've applied over 20 years' of expertise in several safety-critical domains to create a solid, direct approach for solving embedded cyber security problems. CRITICAL Software complies firmly to all relevant standards, guidelines and policies, including:

- ISO/IEC 15408
- ISA/IEC 62443 (the successor of ISA-99)
- ISO/IEC 27000 group of standards
- ETSI, NIST, OWASP, CISQ
- The UK's NCSC policy