Welcome to the First Issue of a New Journal!

Welcome to the launch issue of the Safety-Critical Systems eJournal, which is published by the Safety Critical Systems Club, a UK Community Interest Company. Our mission is, "To publish high-quality, peer-reviewed articles on the subject of systems safety". By systems, we mean not only the platforms, but also the people and their procedures that make up the whole. Systems safety addresses those systems, their components, and the services they are used to provide. We do not have a narrow view of system safety, however; our scope is wide, and includes safety-related topics such as resilience, security, public health, and environmental impact.

This is not *purely* an academic journal presenting research results, we also intend to report upon practical aspects of systems safety; what works and what does not. The aim is to reflect how industrial practise is developing, for example how new standards are to be interpreted, or what new analysis techniques are being trialled. We are also interested in the past, how tools and techniques were justified for deployment, or significant lessons learned (and acted upon); and in the present, with topical or industry review articles, for example.

There will be two issues per volume, published in January and July of each year. In addition to the on-line presentation, each Volume of the journal will be made available in printed form both for libraries and for those of us who want a more-permanent record. The print volume will be published each December.

If you would like to submit a paper for a future issue, please see "Information For Authors" in the right-hand pane of the journal home page.

In this issue we have three papers:

- Rob Ashmore & James Sharp (UK) propose a set of generic assurance topics applicable to all types of programmable content for all types of platform, giving some novel examples;
- Dewi Daniels & Nick Tudor (UK) claim that many software reliability models do not provide results in which sufficient confidence can be placed, proposing an alternative approach; and
- Bruce Hunter (Australia) discusses how cyber-attacks, such as a ransomware attack on a business system, may also affect critical infrastructure, whether intentionally, or unintentionally; he considers cybersecurity threat mitigation, minimising the impact of attacks on safety systems.

My thanks go to the authors for contributing these papers, and also to the peer-reviewers (four per paper) for suggesting improvements. Apologies also to those reviewers who made some recommendations that were not taken up.

You may find some of this material controversial, or you may think that it does not go far enough. Subsequent issues of this journal will have provision for readers' letters to the Editor responding to individual papers.

For more resources addressing system safety, see the Club's web-site https://scsc.uk and please support us by becoming a member.

John Spriggs, Editor

January 2022

About the Cover

The lighthouse, depicted here by Alex King as an island of stability in a stormy sea, represents a safety-critical system, which is intended to provide stable, trusted outcomes in a chaotic environment.

Lighthouses provide help to seafarers and have done so for thousands of years. Some warn of the presence of rocks or of other long-term hazards to navigation. Others are navigational aids and, with other cues, may be used to find a safe passage to harbour. Many perform both rôles; the lighthouse is thus itself (part of) a safety-critical system.