01 Jan 2006

International Working Group on Assurance Cases (For Security)

S. Guerra

M. Masera

Ann K. Miller
Missouri University of Science and Technology

C. B. Weinstock

et. al. For a complete list of authors, see https://scholarsmine.mst.edu/ele_comeng_facwork/1693

Recommended Citation

S. Guerra et al., "International Working Group on Assurance Cases (For Security)," *IEEE Security and Privacy Magazine*, Institute of Electrical and Electronics Engineers (IEEE), Jan 2006.
The definitive version is available at https://doi.org/10.1109/MSP.2006.73

International Working Group on Assurance Cases (for Security)

Robin E. Bloomfield
City University, London

Sofia Guerra
Adelard

Marcelo Masera
European Commission's Joint Research Centre

Ann Miller
University of Missouri, Rolla

Charles B. Weinstock
Software Engineering Institute

Critical systems are aptly named—from electric power to water and gas to the telephone system and the Internet, they're all critical to some aspect of our daily lives. We're a networked society and, as such, it's important to both know whether critical systems are trustworthy and be able to communicate, review, and debate the level of trust achieved in them. In the safety domain, explicit *safety cases* are increasingly required by law, regulations, and standards. (We define a safety case as "a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment."[1]) Increasingly, regulatory agencies are making the case for a goal-based approach, in which claims (or goals) are made about the system, and arguments and evidence support those claims. This approach[1–3] goes back at least a decade, and was heavily influenced by Stephen Toulmin's early work and by the contemporary perspective of proof as a social process.[4,5]

The need to understand risks isn't just a safety issue: organizations must know their risks and be able to communicate and address them for multiple stakeholders, from the boardroom to the back office and beyond. To address these additional sources of risk, researchers are generalizing the ideas behind the safety case into the assurance case. An international community has begun to form around this issue and the challenge of moving from rhetoric to reality. In this article, we outline what a small, international group of experts, spanning various disciplines in safety, security, reliability, and critical infrastructure, has been doing with the International Working Group on Assurance Cases (for Security), what we hope to achieve, and where we go next.

The first step

One of the first public events this international community organized was a workshop entitled, "Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities," which was part of the International Conference on Dependable Systems and Networks held in Florence, Italy, June 2004. Chuck Howell (Mitre), Shari Lawrence Pfleeger (RAND Corp.), Victoria Stavridou-Coleman (SRI International), and Sofia Guerra (Adelard) organized the workshop to promote communication among groups that were working in the broad area of assurance cases. These groups were often unaware of what other, similar groups were doing, so discussions focused on the challenges and opportunities for assurance cases, with the additional aim of initiating the development of a standard set of best practices and guidelines for developing and assessing assurance cases.

Speakers came from Adelard, the City University of London, Mitre, Pfleeger Consulting Group, Praxis Critical Systems, RAND Corp., SKI (the Swedish Nuclear Power Inspectorate), SRI International, Carnegie Mellon's Software Engineering Institute (SEI), and the University of York. The full set of position papers and presentations is available at www.aitcnet.org/AssuranceCases/agenda.html.

An important result of the workshop was the decision to take this work further in the security area; accordingly, Robin Bloomfield (City University London and Adelard), O. Sami Saydjari (Cyber Defense Agency), and Chuck Weinstock (SEI) organized a workshop on assurance cases for security in June 2005, which SEI hosted in Washington, DC. Many of the same individuals who participated in the first workshop attended this follow-up workshop.

Assurance cases for security

The follow-up workshop, called the "Workshop on Assurance Cases for Security," brought together people working on assuring safety, reliability, and security to envision how assurance cases for security ought to work and how the community might pursue viable technical approaches to realize that vision. An

international mix of security and safety practitioners and researchers from Adelard; Cyber Defense Agency; MITRE; SEI; the UK's Defense Science and Technology Laboratory (DSTL); CERT; the University of Missouri, Rolla; City University (London); York University; Carnegie Mellon; SKI; the University of Illinois at Urbana-Champaign; and the European Commission's Joint Research Center (JRC) represented the intersection of several communities.

The workshop's overall objective was to assess how to develop assurance cases for security and what challenges such activities presented. It produced the following outputs:

- a vision statement, including what the workshop attendees hoped to achieve with assurance cases and what difference it would make if we were wildly (or even moderately) successful;
- a top-level decomposition of the problems associated with developing assurance cases;
- a mapping of existing work to the decomposition;
- a set of key hard problems and promising approaches;
- a list of possible research sponsors for assurance cases; and
- some worked examples.

The workshop started with introductory talks and discussions on safety cases and security assurance, followed by parallel sessions in which three groups constructed example fragments of assurance cases for security (the previously mentioned safety cases) based on a common model. Ann Miller (University of Missouri, Rolla) offered a three-layer model of a robot manufacturing facility, with a supervisory control and data acquisition (SCADA) layer and a corporate intranet. The groups used this model to explore the differences between security and safety cases, and to learn what works and what doesn't in a security context.

The workshop's overall aim was to investigate possible answers to some key issues:

- *Claims*. Are there standard patterns for claims about certain kinds of properties or systems? Are these claims sufficiently tangible to be subjected to rigorous assurance cases? How can organizations elicit appropriate claims from stakeholders?
- *Arguments*. What makes an assurance case "compelling"? Are there standard patterns for arguments? Do different audiences have differing criteria, and are some criteria better than others? What arguments should be compelling, and what arguments do people actually find compelling? How do additional arguments or evidence increase a case's compelling nature? If accepted notions make a case compelling, to what extent do we know that these accepted notions are correct?
- *Evidence*. What evidence is needed to support an argument? What new types of evidence are needed to create more sound arguments? By what metrics do we assess the effectiveness of evidence?
- *Justification*. What is the cost–benefit justification for developing an assurance case? Are there different levels of effort, depending on motivation? Can we quantify these levels? What short-term benefits arise from assurance case activity? Can we show that a well-defined and executed assurance case process will cost less than current assurance processes?
- *Maintenance*. How are assurance cases maintained as systems evolve?
- *Composition*. How can assurance cases be composed?

A recent report (www.csr.city.ac.uk/AssuranceCases) provides the workshop's technical output; it concentrates on the results of the three breakout groups, which generated very different and somewhat complementary results. The report's conclusion section summarizes the discussion on the way forward.

A key lesson from the workshop was how the participants' different backgrounds and perspectives proved to be mutually stimulating and informative. The more safety-oriented participants also recognized that, even though many technical issues must be addressed and safety tools and notations can be deployed on security, the underlying methods still must be developed. The lessons learned and issues raised include

- describing how hierarchical conceptual decomposition puts security requirements in context;
- acknowledging the need to address all attributes, terminology, and concept issues;
- declaring "open season" on arguments and leaving it to the users to define them;
- determining the balance between inductive and deductive techniques;
- discovering the role of models and the relationships between them;
- examining how the results of vulnerability assessments and attack trees fit into assurance cases;
- determining when to stop and knowing when the case is complete;
- defining the role of standards; and
- learning how to deal with the

A key lesson from the workshop was how the participants' different perspectives proved to be mutually stimulating and informative.

need for both trusted and trustworthy cases.

The workshop concluded with the determination to continue the series into assurance cases for security.

Trust and risk communication in critical infrastructure

In March 2006, the series continued with a workshop entitled, "Assurance Cases for Security: Communicating Risks in Infrastructures," hosted by the European Commission's JRC in Ispra, Italy, and organized by Marcelo Masera. The event brought together the core group who attended the previous workshops along with experts in risk assessment and communication. Importantly, it included a practitioner from a critical UK nuclear infrastructure who was responsible for justifying information and communications technology (ICT) system security.

The important conclusion from this workshop was the need to support the communication of risks between stakeholders involved in critical infrastructures; assurance cases appear to be a workable solution. They can be applied to the different types of objects that compose an infrastructure, from products to processes to systems to organizations. The assurance cases for different types of objects might exist for different objectives, take different shapes, and obtain evidence from very different sources, but we believe it might be possible to develop a common theoretical and methodological support for all assurance cases.

Assurance cases can be motivated by regulations (laws, standards, and codes of practice), internal decisions made by owners or producers, and bilateral agreements (or contracts). This multiplicity of objectives can affect the negotiations and trade-offs in assurance case claims—and, more important, to the interpretation of an assurance case's results.

Because critical infrastructures and process control systems are dynamic with changes in configuration caused by connectivity, software updates, and other business issues, their assurance cases are more dynamic because they must be reviewed when new information comes in about system vulnerabilities or threats, or when the system's structure, functioning, or behavior change. Consequently, the assurance case's validity is in constant flux. This fact creates a specific dynamic in a system's evolution from trustworthy to trusted.

The workshop also further developed some of the observations from previous workshops, especially about the need for argument composition to incorporate rationale and evidence from different sources. The multiplicity of stakeholders requires us to manage different views on an assurance case (for example, specific claims and details in arguments and evidence). In multiparty settings, the assurance case plays a key role in risk-related decision-making processes, which might be performed in very different styles (such as adversarial or collaborative).

These various workshops have identified several technical, policy, and research challenges that policy makers, practitioners, and the research community must solve; fortunately, we're working collectively and individually to address them. We are currently developing more considered technical publications from workshop reports and planning further activities. If you're interested in collaborating or participating, please contact Robin Bloomfield (reb@csr.city.ac.uk). □

References

1. R.E. Bloomfield et al., *ASCAD—Adelard Safety Case Development Manual*, Adelard 1998.
2. P.G. Bishop, R. Bloomfield, and S. Guerra, "The Future of Goal-Based Assurance Cases," *Proc. Workshop on Assurance Cases*, 2004, pp. 390–395.
3. T. Kelly, *Arguing Safety: A Systematic Approach to Managing Safety Cases*, PhD thesis, Univ. of York, 1998.
4. S.E. Toulmin, *The Uses of Argument*, Cambridge Univ. Press, 1958.
5. D. MacKenzie, *Mechanizing Proof: Computing, Risk and Trust*, MIT Press, 2001.

Robin E. Bloomfield *is director of the Centre for Software Reliability at the City University, London, where he's also a professor of software and system dependability. His research interests are in the dependability (reliability, safety, security) of sociotechnical systems. Bloomfield has a degree in natural sciences from Cambridge University. Contact him at reb@csr.city.ac.uk*

Sofia Guerra *is a partner at Adelard. Her technical interests include the safety and reliability of computer-based systems. Guerra has a PhD in mathematics from Lisbon Institute of Technology (IST), Portugal. Contact her at aslg@adelard.com.*

Marcelo Masera *is a scientific officer of the European Commission's Joint Research Centre. His technical interests include security of critical infrastructures, and risk assessment and governance. Masera has a degree in electronics and electrical engineering from the University of Mendoza, Argentina. Contact him at marcelo.masera@jrc.it.*

Ann Miller *is the Cynthia Tang Missouri Distinguished Professor of Computer Engineering at the University of Missouri, Rolla. Her technical interests include security and reliability of large-scale networked systems. Miller has a PhD in mathematics from Saint Louis University. She is a senior member of the IEEE and the IEEE Computer, Communications, and Reliability Societies. Contact her at annmiller@ieee.org.*

Charles B. Weinstock *is a senior member of the technical staff in the Performance Critical Systems Initiative at the Software Engineering Institute at Carnegie Mellon, where he specializes in dependable systems and assurance cases. He has a PhD in computer science from Carnegie Mellon. Weinstock is a senior member of the IEEE. Contact him at weinstock@sei.cmu.edu.*