INSTITUTE FOR DEFENSE ANALYSES

Review of Potential Assurance Case Tool Options for DoD

Kevin P. Roback

Revised January 2024
Approved for Public Release.
Distribution Unlimited.
IDA Publication D-33524 /2
Log: H 2024-000007

INSTITUTE FOR DEFENSE ANALYSES 730
East Glebe Road
Alexandria, Virginia 22305

Distribution Statement A: Approved for public release; distribution is unlimited.

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project AX-01-3100, "DTE&A Initiative," for the Director, Developmental Test Evaluation and Assessments. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

The authors would like to thank the IDA committee, Dr. Stephen Ouellette (chair), Dr. Rachel Kuzio. de Naray, Mr. Christopher A. Martin, Dr. Daniel G. Shapiro, and Dr. David M. Tate for providing technical review of this effort.

For More Information

John S. Hong, Project Leader
jhong@ida.org, 703-845-2564

Stephen M. Ouellette, Director, SED
souellet@ida.org, (703) 845-2443

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

Distribution Statement A: Approved for public release; distribution is unlimited.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-33524 /2
Revised January 2024

Review of Potential Assurance Case Tool Options for DoD

Kevin P. Roback

Distribution Statement A: Approved for public release; distribution is unlimited.

Distribution Statement A: Approved for public release; distribution is unlimited.

Executive Summary

Assurance cases (ACs) can improve the safety assurance process for many systems; their structured, visual argument form links claims about a system visually to arguments supporting the claim, and evidence supporting the argument. However, complex systems require complex assurance cases, which can take a great deal of time and effort to construct. To assist with this difficulty, numerous practitioners in industry and academia have created tools for assurance case development. The large number of tools can be a source of confusion for new practitioners; in our previous work (Roback, Sparrow and Tate 2022) we documented 46 known assurance case tools from the open literature. A minority of these (22 of 46) are available for public use.

In this follow-on study, we attempt to directly access and use the tools we previously judged to be available, evaluating ease in set up and initial use, and cybersecurity. Our previous study documented that many assurance case tools, particularly open-access tools, were the products of now-discontinued projects by small groups of academic researchers. This follow-on review makes the limitations of these open source tools clearer; many are not well documented nor easy to install and use. Many depend on external software packages, which can also be difficult to install and operate. Many packages introduce cybersecurity issues due to known vulnerabilities in the software, histories of the software being used as a vector in cyberattacks, conflicts between the software's security protocols and organizational security protocols, and concerns arising from connections between the software's developers and companies targeted by U.S. Government restrictions.

Due to these limitations, we found that only one open-access tool (D-Case Weaver) out of 17 investigated could be seriously considered for use in Department of Defense (DoD) computing environments at this time. That tool offers relatively basic capabilities relative to other, less-accessible tools. Aside from open-access tools, commercial assurance case tools are also available. We investigated seven commercial tools, with the goal of obtaining demonstrations and trial versions where possible. Though one commercial tool turned out to be discontinued, and one was entirely unsuitable for DoD use due to a cloud-based infrastructure, the other tools were generally easier to install and use than their open-access counterparts. Overall, they are better documented, with more functionality as well; some providers even offer training courses.

Our work shows the importance of cybersecurity issues in assurance case tool selection. It is worth noting that, though we find fewer *apparent* issues with the security of commercial tools relative to the security of open source tools, this may in part arise from

the fact that open source tools are more transparent; anyone can access the code, and information about how the tool was built is generally made public, and not kept confidential or proprietary. Dependencies on external software packages were the main cause of security problems regarding open-source tools. Similar issues may also exist (but be less obvious) in commercial tools, as most commercial tool providers did not offer freely downloadable trial versions of their products. Live demos over a remote call were more commonly offered.

Though multiple credible commercial options are available, the cybersecurity challenges with existing tools raise the question of whether in-house tool development may be worthwhile to lessen cybersecurity concerns. An in-house development effort may face challenges in funding and staffing. The results of such an effort also may not necessarily be accessible and used widely in DoD, and may not eliminate cybersecurity concerns, especially if open source software packages are used to expedite development.

Finally, we investigated assurance case tools' linkages to MBSE (model-based systems engineering) tools. This topic is of some interest, as MBSE diagrams contain information about a system that may be machine readable, and incorporated into an assurance case. Though some assurance case tools do provide some level of capability to also model a system's architecture, in general MBSE is not prioritized or heavily mentioned in existing assurance case tools, with the exception of one tool (Astah System Safety).

Contents

(This page is intentionally blank.)

1. Introduction

Assurance cases (ACs) are structured arguments which demonstrate that a system is sufficiently trustworthy for a particular intended use. Assurance cases are commonly organized as branching, upside down tree-like diagrams following one of two formalisms. The oldest formalism is known as Claims-Argument-Evidence, or CAE. The goal of an assurance case is to confirm a top-level claim about the system (e. g., "the system is safe"). Claims can be supported by sub-claims, which are supported by arguments; these arguments are supported by evidence. An alternative notation that has been developed more recently is Goal Structuring Notation (GSN); it is largely the same as CAE, but uses different terms to refer to its components. CAE claims become "goals", arguments are "strategies" and pieces of evidence are "solutions".

Constructing these arguments can become complicated given the complexity of modern software & hardware systems, and the number of hazards and possible failure modes that these systems may experience. In particular, the number of sub-claims, arguments and pieces of evidence in an assurance case can be significant. To ease the process of building these arguments, assurance case practitioners in industry and academia have created a variety of tools. In previous work (Roback, Sparrow and Tate 2022), we updated a pre-existing (Maksimov, et al. 2018) survey of these tools with information on new tools, and additional information collected on already-known tools. This report builds on that previous work.

In our previous survey, we reported on 46 assurance case tools, discovered through the pre-existing Maksimov, et al. 2018 survey, and conducted our own additional searches in the safety case, assurance case, and cybersecurity literature. We determined the availability of these tools, characterizing them as being either open-access (the tool could be accessed and used without payment), paid access or unavailable. Many tools discussed in the open literature turned out to be unavailable (20 of 46); many had been discontinued, or were produced by old research projects that never reached completion or public release. The availability of an additional four tools could not be determined, leaving us with a list of 22 available assurance case tools for further evaluation. Since our previous paper, we also identified two new assurance case tools that were released, to bring the total number of known tools to 24. Our previous study re-used a rubric developed by Maksimov, et al. 2018 to evaluate the relative capabilities of these 24 assurance case tools. These evaluations were not based on actual work with the tools, but on their capabilities as stated in the papers/documentation published about them. This preliminary evaluation identified a group of tools with relatively strong advertised capabilities, but did not address some

important issues, such as the cybersecurity of the tool itself, the quality of the tool's documentation, and the ease of tool installation and use.

We address these issues in this follow-on work by attempting to directly access, download and use each tool found by our previous survey. We also investigate the extent to which tools may be used as part of a model-based systems engineering (MBSE) framework. In particular, we considered tools' ability to support the creation of system-model diagrams in addition to assurance case diagrams, and the degree of interoperability and data transfer between these frameworks. Section 2 of this work focuses on cybersecurity and usability for open source tools, while Section 3 covers the same issues for commercial tools. Section 4 discusses MBSE constructs in assurance case tools, while Section 5 concludes the paper.

2. Results – Open Source Tools

Our previous survey identified a list of 17 potentially available open source tools. We evaluate each in the categories of cybersecurity and ease of use (Table 1). In the "Cybersecurity" column, green indicates a tool with no known issues; red indicates a tool with issues. The name of the primary software package the tool is built off is provided in this column also. In the "Ease of use" column, green indicates a well documented and easy to install and use tool, while red indicates a tool that is either poorly documented or difficult to install and use; the factors making a tool difficult to use are provided in this column as well. Yellow in this column indicates a tool that would be difficult for most to learn, but easier for people with prior knowledge of the right software packages (these are explained later in this section)

Table 1: Evaluation of cybersecurity and ease of use of open source assurance case tools

Tool Name	Cybersecurity	Ease of use
ACEdit	Eclipse IDE	Eclipse install, documentation, support
AdvoCATE	Eclipse Framework	No major issues
AGSN	Eclipse IDE	Eclipse install, No support
AutoFOCUS3	Eclipse Framework	No major issues
CertWare	Eclipse IDE	Eclipse install, documentation, no support
D-Case Communicator	Web-based	Not in English
D-Case Editor	Eclipse IDE	Eclipse install, no download
D-Case Weaver	No dependencies	No major issues
Eclipse & Papyrus extension	Eclipse IDE	Eclipse install, no download
ENTRUST	Eclipse IDE	Eclipse install, documentation

Evidential Tool Bus	Python 2.7	No support, no GUI, Python
FASTEN	JetBrains MPS	Untested
MMINT-A	Eclipse IDE	Eclipse install, documentation
OpenCert	Eclipse IDE	Eclipse install, documentation
Resolute	Eclipse IDE	Eclipse install, documentation
SafeEd	Eclipse IDE	Eclipse install, no download
VERDICT	Eclipse Framework	OSATE/AADL

As seen in Table 1, only one tool (the Weaver portion of the D-Case suite) is suitable for potential DoD use in its current form. D-Case Weaver was developed by Dependability Engineering for Open Systems (DEOS), a research group that states it receives funding from the Japan Science and Technology Agency (DEOS n.d.). D-Case Weaver enables intuitive manual construction of assurance arguments, but lacks the more detailed hazard and system modeling capabilities of more developed tools. It is easy to install and run and raises no obvious cybersecurity issues, so it may be suitable for DoD use. The other sixteen tools were found to be unsuitable due to cybersecurity issues or overly difficult onboarding processes associated with using the tools.

1. Cybersecurity

The greatest cybersecurity issue we identified resulted from the fact that most (13 of 17) of the open source tools operate using tools from the Eclipse Foundation. Ten of these 13 require a full installation of the Eclipse IDE (Integrated Development Environment) to operate. Others do not require a full installation of the IDE, but nonetheless install and use many Eclipse-produced frameworks, such as the Eclipse Graphical Editing Framework, the Eclipse Modeling Framework, and the Eclipse Rich Client Platform.

We have deemed Eclipse-based tools as an unacceptable security risk due to several factors. Some of these relate to the Eclipse IDE's networking protocols, which create conflicts between Eclipse IDE and common corporate and government cybersecurity protocols. In particular, such networks commonly use security stores embedded in the operating system of the computer, and managed by organizational cybersecurity staff.

Eclipse, however, uses its own security store, which must be patched to accommodate the organization's proxy certificates before Eclipse IDE can be installed.

The process to patch Eclipse IDE's security store is arduous, and official instructions from Eclipse IDE developers could not be found. Eclipse certificate management is a complicated affair requiring experts with deep knowledge of Eclipse and Java. This problem affects the 10 tools that require installation of the Eclipse IDE to function.

Further investigation and review identified other issues that affect the remaining three (of 13) tools that do not require full installation of the Eclipse IDE, but that nonetheless use Eclipse frameworks to operate. These issues included possible collections and storage of data in the "cloud" by functions within the Eclipse IDE, and a connection between the Eclipse Foundation's Board of Directors and Huawei Technology Corporation of China; in particular, Huawei Technology Corporation's Chief Strategy Officer sits on the Eclipse board. Huawei has extensive connections to the Chinese Communist Party, including sustained financial support and orders under Chinese intelligence laws to assist with Chinese military and government intelligence collection requests (Federal Communications Commission 2020).

Though the influence of Huawei within Eclipse is uncertain (only one of the 25 members of the Eclipse Foundation's board of directors is from Huawei), this issue, taken in context with the aforementioned installation and networking issues in Eclipse software, provides reason to avoid tools that build off the Eclipse framework.

Some other non-Eclipse-based tool also had significant cybersecurity issues. FASTEN (Carlan and Ratiu 2020) was developed by German authors with connections to the research group responsible for AutoFOCUS3. Unfortunately, FASTEN is unsuitable for DoD use as it runs from software (JetBrains MPS) currently under investigation for its role in a major security breach. As of January 2021, JetBrains was thought to have been used as a vector by Russian hackers in the SolarWinds hacking episode (Perlroth, Sanger and Barnes 2021).

A different cybersecurity issue affects D-Case Communicator; the tool is a Web-based tool, so it is not suited for classified or CUI content. The Evidential Tool Bus is based around Python 2.7, which is not known to have any significant cybersecurity issues. D-Case Weaver is a standalone tool not requiring the addition of other software packages. It also has no known issues.

2. Ease of Installation and Use

We also examined the ease of use of all of the open source tools. Some tools were found to be unavailable, with non-functioning download links; these included D-Case Editor, the Eclipse & Papyrus extension tool, and SafeEd. Other tools had issues with documentation – it was often either not detailed, or not clearly organized. Tools with

documentation issues included ACEdit, CertWare, ENTRUST, MMINT-A, OpenCert, Resolute, and VERDICT. For VERDICT, we note that the tool may be easier to learn for people who have experience with the software distribution OSATE, and familiarity with AADL (the Architecture Analysis and Design Language) – the documentation assumes prior familiarity with both, providing a challenge for newcomers.

Some tools were outdated and appeared to no longer be supported by their authors – ACEdit, AGSN and CertWare sit on Github-type repositories that have seen no activity in more than five years. AdvoCATE and AutoFOCUS3, which were the most capable of the open-source tools we evaluated, had no issues with availability, installation, documentation, or lack of current support – those tools are not recommended due only to the aforementioned issues with Eclipse Foundation software. FASTEN was also well documented, but given the more serious and demonstrated issues with JetBrains MPS, we elected to not test the software in full.

The Evidential Tool Bus (Cruanes, et al. 2013) applies a variety of formal methods to assurance case tool evaluation. This tool is a set of Python packages that only works on Python 2.7.x (not the modern Python 3.x). Setting this tool up will therefore require most users to set up a new Python environment on their machine. The assurance cases are also set up in the tool via lines of Python code, rather than graphically as with almost all other tools. However, the procedures for setting it up are fairly well documented (Owre and Mason 2016). The tool was last updated in 2016. In general, the dependency on old versions of Python and lack of graphical representation of assurance cases make this tool a poor option for those inexperienced in Python.

Lastly, D-Case Communicator is unsuited for DoD use as its menus and instructions are in Japanese. D-Case Weaver is in English, however, and it is clearly documented and easy to install and use.

3. Results – Commercial Tools

Our prior survey identified five available commercial assurance case tools. Further interaction with the assurance community led us to nLoop, a tool produced by Edge Case Research Inc., and Socrates, a tool produced by Critical Systems Labs. Our evaluation of cybersecurity and ease of use for these seven commercial tools is summarized in Table 2. The symbology mirrors that of Table 1, with the exception that we left boxes white in the "Cybersecurity" column if we were unable to access them for evaluation. More details on each tool are provided in the subsequent text.

Table 2: Evaluation of cybersecurity and ease of use for commercial assurance case tools.

Tool Name	Cybersecurity	Ease of use
ASCE	No known issues	No major issues
Astah System Safety	No known issues	No major issues
ISCaDE	Unavailable for trial	No download
nLoop	No known issues	No major issues
NOR-STA	Web-based	No major issues
Socrates	No known issues	No major issues
TurboAC	Unavailable for trial	Untested

The Assurance and Safety Case Environment (ASCE), is produced by Adelard, a UK-based company that is part of a software development group called NCC Group. Adelard has been involved in developing tools for assurance case creation since the early 2000s (Emmet and Guerra 2005). ASCE continues to be updated, with the most recent release (ASCE 5.1) arriving in 2022 (NCC Group 2022). We reached out to the developers and were given a live demo of ASCE, but not a full trial version to evaluate – in the demo, the intuitive user interface for tool building, enabling quick construction of assurance case arguments was made apparent. The tool contains limited capability to compute confidence levels automatically, or automatically reference and update assurance cases to reflect changing data. Adelard offers training in ASCE, but costs are not stated up front – the costs of licensing the software are not stated publicly, either. 30-day free trials of the software are advertised for interested users. Adelard has experience working with defense-industry

clients (NCC Group 2024). ASCE's only software dependencies are Microsoft packages, such as Microsoft Office and Visual Studio C++, which are widely used in DoD.

Astah GSN was developed by ChangeVision, Inc., a company based in Japan. It is now being discontinued in favor of the more capable Astah System Safety tool that ChangeVision has more recently produced; the rest of this discussion will focus on Astah System Safety. Astah System Safety improves upon Astah GSN, which was a standard Goal Structured Notation (GSN) editor for assurance case construction, by integrating the assurance case capabilities with support for other aspects of system development and engineering – in particular, MBSE. The core GSN-building part of Astah System Safety is directly carried over from Astah GSN with no changes. For GSN diagramming, the Astah System Safety documentation page, as of May 2023, redirects users to Astah GSN documentation (ChangeVision, Inc. 2015).

Astah System Safety supports the creation of SysML diagrams in addition to conventional GSN diagrams (ChangeVision, Inc. 2023). Similarly to other commercial tools, construction of assurance cases is simple, with an easy to operate graphical user interface. ChangeVision, Inc. offers a 40-day free trial of Astah System Safety, and organizational and individual pricing for licenses are provided up front on the Astah website.

ISCaDE was a tool developed by a firm called "rcm2 limited", whose website implies it is a UK-based firm (given its ".co.uk" address), and claims to have been in business since 1998. However, no contact address is provided and no specific authors are named on the tool website (rcm2 limited 2014). Links to a trial version of ISCaDE exist on the firm's website but turned out to be nonfunctional when we tried to follow them. Furthermore, the firm's website does not appear to have been updated since 2014. No other working ISCaDE webpage could be located, giving the appearance that the firm producing this tool no longer exists.

Edge Case Research, Inc. is developing a tool called nLoop. Edge Case provided a demo of the tool, which focuses heavily on "live safety cases" that automatically propagate the effects of changes to the argument or evidence through the rest of the safety case; a focus on facilitating multiuser collaboration is also a priority. Specifics about the tool are not posted publicly; one must request a demo on the Edge Case website (Edge Case Research, Inc. 2022) to learn more. Edge Case has experience working with the U. S. defense industry (Edge Case Research, Inc. 2021). Though we were unable to access a full demo for the tool, its developers state that it does not require Eclipse nor Jetbrains software to run.

Argevide, a software consulting company established in 2014 in Poland, developed a tool called NOR-STA. NOR-STA is Argevide's main product, and has been updated annually with new features since 2014 (Argevide 2023). It is a web browser-based online

GSN editor in which an assurance case is constructed in a thread-like manner, with goals identified first and then subgoals, strategies, claims and evidence instantiated as insets to goals; a graphical editor then automatically lays out a graphical assurance case from these threads, which often requires manual editing. The construction and editing process are explained in straightforward ways through online tutorial videos, and a detailed online user's manual. However, the cloud-based nature of the tool means that it cannot be used with CUI or classified information, making NOR-STA a poor fit for DoD use.

Critical Systems Labs, a company based in Canada, recently released a tool called Socrates (Critical Systems Labs, Inc 2024), with further updates through 2023 and into 2024. Critical Systems Labs's tool is generalizable to various kinds of argument formation, including structures such as GSN, and an extension to GSN developed by Critical Systems Labs, called Eliminative Argumentation (EA) (Critical Systems Labs, Inc. 2020). EA is a framework focused more on disproving a lack of safety, than proving safety, motivated by its creators' concerns about affirmative confirmation biases in safety case construction.

Socrates has a server-based infrastructure, in which critical files are hosted on a server, and administrators can control access and permissions for users to collaboratively build an argument for system safety. This infrastructure can be flexibly hosted on a private server, enabling the tool to protect sensitive information. Various features have been developed to improve ease of use. Rules, which can be customized by users, can automatically check argument completeness. Data can be uploaded automatically via API to update an assurance case's argument. Custom controls on argument views can be used to protect sensitive information, and customize views to fit various stakeholders' interests. Though we did not have access to a fully downloadable demo, the tool developers do state that their software package is intended to be self-contained, with the only claimed external dependency being MySQL, which is widely used in the DoD. An online trial version of the software is available through Critical Systems Labs's webpage.

GessNet, a U.S. based software company, produced the tool suite TurboAC (GessNet 2023). Since the previous survey, GessNet has released an updated toolset called QMSpace. GessNet's products are heavily geared toward medical device assurance; the company's mission/vision statements all mention medical devices specifically, and not other kinds of devices. Though an initial response from the company implied a level of interest in applying their tool for defense-related systems, we have not heard back from the company since then and have not been able to access a demo or trial version.

(This page is intentionally blank.)

Distribution Statement A: Approved for public release; distribution is unlimited.

4. MBSE Integration

MBSE (model-based systems engineering) uses models, in lieu of text descriptions, to represent aspects of a system's design including its hardware, software, functions, requirements, and more. Models can include diagrams showing how parts of a system will interact with one another and the environment. They also will include physics-based numerical models used to predict a component's behavior. Other authors (Evans, Cornford and Feather n.d.), (Biggs, et al. 2018)) have written at length about the potential value to be gained from combining MBSE approaches with assurance case construction. However, these papers do not dive into specifics or mechanics of how information generated in the MBSE context should be integrated with assurance cases. For this study, we noted tools that had capabilities to model system architecture through commonly used MBSE formalisms such as SysML. Though this architectural modeling does not, in itself, constitute MBSE (MBSE also involves numerical modeling of system component behaviors), such frameworks are an important part of the practice.

Astah System Safety (ChangeVision, Inc. 2023) explicitly promotes linkage between the MBSE and assurance case methodologies. It supports creation of SysML diagrams, as well as some interoperability between SysML diagrams and GSN (Goal Structuring Notation) diagrams, with conversions of SysML blocks to GSN solutions, and SysML requirements to GSN goals. SysML is a commonly used system modeling notation in MBSE, so the ability to support both MBSE and assurance frameworks in one tool, as opposed to acquiring separate tools for both, could hypothetically improve efficiency. However, SysML diagrams and assurance case diagrams inherently involve artifacts that are different from one another; thus, they have limited ability to transfer information from one context to another.

No other assurance case tool potentially suitable for DoD use that we evaluated integrates MBSE capabilities explicitly, though some, such as Socrates, have generalized argument structures that could be used to build an MBSE model.In general, MBSE and assurance case tools exist in separate worlds. Writeups and documentation for assurance case tools rarely mention MBSE, though some tools do have system-modeling capabilities not referred to as "MBSE". AutoFOCUS3 includes some system-modeling capabilities (fortiss 2022). The ENTRUST methodology (Calinescu, Weyns, et al. n.d.) calls for assurance cases to be developed in parallel with models of the system, but this is not referred to as MBSE. Though, as mentioned earlier, authors are writing in the abstract about MBSE's potential benefits for assurance case construction, assurance case tools, with Astah System Safety's exception, are generally not prioritizing linkages to MBSE.

(This page is intentionally blank.)

5. Summary and Conclusions

Through our prior 2022 survey and continued engagement in 2023, we identified and evaluated a total of 24 assurance case tools thought to be available and potentially suitable for DoD use. We assessed each tool in the categories of cybersecurity, ease of installation and use, and MBSE integration. Through hands-on work with the tools, involving attempts to install the tools and the external software packages they depend on, we found a litany of issues that make most tools unsuitable for defense work. These issues generally revolved around cybersecurity, though usability and onboarding, particularly for open-access tools, was also a challenge. Of the 17 studied open access tools, only one, the Weaver portion of the D-Case suite, was found to be potentially suitable for official Department of Defense use at this time – and it has relatively 'bare-bones' capabilities.

Fewer apparent issues were found for commercial tools, though we were unable to work with as many of the commercial tools directly. Very few tools in general support the integration of assurance case and MBSE frameworks; Astah System Safety is the only tool that we evaluated that explicitly links assurance case and MBSE methodologies. It also lacks any obvious cybersecurity issues, making it a credible commercial option. Other potential choices in the commercial sphere include nLoop, Socrates, and ASCE, which are all produced by vendors who have worked with defense clients previously..

Though credible commercial options are available, the cybersecurity challenges raise the question of whether the successful adoption of the assurance case methodology across DoD requires investment in the in-house development of assurance case tools. The Test Resource Management Center (TRMC) has experience in software development for testing; one tool produced by TRMC, known as SAFE, automates assurance case evaluation under some safety standards, so TRMC has some prior assurance case experience. However, any government software development effort will have to contend with typical government challenges of attracting and retaining high-level talent, and getting a disparate base of potential users to actually apply developed tools in their operating environments.

(This page is intentionally blank.)

Appendix A. Bibliography

Argevide. 2023. *Argevide: About us.* Accessed Jan 9, 2024. https://www.argevide.com/about-us/.

Barry, M. R. 2011. "CertWare: a workbench for safety case production and analysis." *Proceedings of Aerospace Conference 2011.* 1-10.

Biggs, G., A. Armonas, T. Juknevicius, and K. Post. 2018. "Integrating Safety and Reliability Analysis into MBSE: overview of the new proposed OMG standard." *INCOSE International Symposium.*

Calinescu, R., D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly. n.d. *Engineering Trustworthy Self-Adaptive Software.* Accessed April 13, 2023. https://www-users.york.ac.uk/~sg778/ENTRUST/.

Calinescu, R., D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly. 2017. "Engineering trustworthy self-adaptive software with dynamic assurance cases." *IEEE Transactions on Software Engineering* 1-30.

Carlan, C., and D. Ratiu. 2020. "FASTEN.Safe: A Model-driven Engineering Tool to Experiment with Checkable Assurance Cases." *SAFECOMP 2020.* Springer.

Carnegie Mellon University. 2023. *Welcome to OSATE.* Apr 17. Accessed Apr 28, 2023. https://osate.org/.

ChangeVision, Inc. . 2015. "Astah GSN Quick Start Guide." *Astah GSN Tutorial.* Accessed May 4, 2023. https://s3.amazonaws.com/cdn.astah.net/resources/Astah+GSN+Start+Guide.pdf.

ChangeVision, Inc. 2023. *Astah System Safety.* Accessed Jan 9, 2024. https://astah.net/products/astah-system-safety/?utm_campaign=products&utm_source=product-list-asy-by-sysml&utm_medium=asy-by-sysml.

—. 2023. *Support for Astah GSN - Help documentation for Astah.* Accessed May 3, 2023. https://astah.net/support/astah-gsn/.

Collins Aerospace. 2022. *loonwerks/Resolute.* Aug 30. Accessed Apr 20, 2023. https://github.com/loonwerks/Resolute/releases.

Critical Systems Labs, Inc. 2024. *Socrates Assurance Case Editor.* Accessed Jan 12, 2024. https://criticalsystemslabs.com/socrates/.

Critical Systems Labs, Inc. 2020. *Why Use Eliminative Argumentation.* May 15. Accessed Jun 8, 2023. https://criticalsystemslabs.com/resources/blog/14-nlogcontent/54-why-use-eliminative-argumentation.

Cruanes, S., G. Hamon, S. Owre, and N. Shankar. 2013. "Tool integration with the evidential tool bus." *VMCAI 2013.* Springer: Heidelberg. 275-294.

Denney, E., and G. Pai. 2018. "Tool support for assurance case development." *Autom Softw Eng* 435-499.

DEOS. n.d. *D-Case Weaver.* Accessed March 31, 2023. https://www.jst.go.jp/crest/crest-os/tech/DCaseWeaver/index-e.html.

—. n.d. *DEOS: About this site.* Accessed March 31, 2023. https://www.jst.go.jp/crest/crest-os/osddeos/en/aboutsite.html.

Despotou, G., A. Apostolakis, and D. Kolovos. 2012. *acedit.* April 16. Accessed April 7, 2023. https://code.google.com/archive/p/acedit/.

Di Sandro, A., G. Selim, R. Salay, T. Viger, M. Chechik, and S. Kokaly. 2020. "MMINT-A 2.0: Tool Support for the Lifecycle of Model-Based Safety Artifacts." *MODELS '20 Companion Proceedings.* no. 15, 1-5.

Di Sandro, A., N. Fung, and N. Murphy. 2023. *Github - MMINT.* Accessed April 25, 2023. https://github.com/adisandro/MMINT.

Edge Case Research, Inc. 2021. *Edge Case Defense.* Accessed Jan 9, 2024. https://www.ecr-defense.ai/.

—. 2022. *Edge Case Research.* Accessed Jan 9, 2024. https://www.ecr.ai/.

Emmet, L., and S. Guerra. 2005. "Application of a Commercial Assurance Case Tool to Support Software Certification Services." *Proceedings of the 2005 Automated Software Engineering Workshop on Software Certificate Management (SoftCeMent '05).* Long Beach, CA, USA: Association for Computing Machinery. 51-55.

Evans, J., S. Cornford, and M. S. Feather. n.d. *Model Based Mission Assurance (MBMA): NASA's Assurance Future.* NASA.

Federal Communications Commission. 2020. "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs - Huawei Designation." Washington, D.C., June 30.

fortiss. 2023. *About fortiss: Gaining the edge through software.* Accessed March 31, 2023. https://www.fortiss.org/en/about-fortiss.

—. 2022. *AutoFOCUS3: Model-based development of embedded systems.* November 17. Accessed March 31, 2023. https://www.fortiss.org/en/results/software/autofocus-3.

Gacek, A., J. Backes, D. Cofer, K. Slind, and M. Whalen. 2014. "Resolute: an assurance case language for architecture models." *Proceedings HILT 2014.* 19-28.

GessNet. 2023. *Medical Devide Safety Assurance Case and Risk Management Solutions.* Accessed Jan 16, 2024. https://www.gessnet.com/.

Górski, J., A. Jarzebowicz, J. Miler, M. Witkowicz, J. Czyżnikiewicz, and Jar. P. 2012. "Supporting assurance by evidence-based argument services." *SAFECOMP 2012.* Heidelberg: Springer. 417-426.

Groza, A., and N. Marc. 2014. "Consistency checking of safety arguments in the goal structuring notation standard." *Proceedings of ICCP 2014.* 59-66.

Huhn, M., and A. Zechner. 2009. "Analysing dependability case arguments using quality models." *SAFECOMP 2009.* Heidelberg: Springer. 118-131.

Larrucea, X. 2016. "Modelling and Certifying Safety for Cyber-Physical Systems: An educational experiment ." *2016 42nd Euromicro Conference on Software Engineering and Advanced Applications (SAEA).*

Larrucea, X., A. Walker, and R. Colomo-Palacios. 2017. "Supporting the management of reusable automotive software." *IEEE Software* 40-47.

Larrucea, X., J. Martinez, A. Lopez, J. Mauersberger, S. Puri, T. Liem Phan, M. Atif Javed, I. Sljivo, and A. Ruiz. 2023. *Eclipse OpenCert.* February. Accessed April 25, 2023. https://gitlab.eclipse.org/eclipse/opencert.

Luo, Y., M. van den Brand, Z. Li, and A. Saberi. 2017. "A systematic approach and tool support for GSN-based safety case assessment ." *Journal of Systems Architecture* 1-16.

Luo, Y., M. van der Brand, Z. Li, and A. Saberi. 2016. "AGSNEditor." *Github.* Dec 5. Accessed Apr 20, 2023. https://github.com/AGSNeditor/development.

Maksimov, M., N. L. S. Fung, S. Kokaly, and M. Chechik. 2018. "Two Decades of Assurance Case Tools: A Survey." *SAFECOMP 2018 Workshops.* Springer. 49-59.

Meng, B., D. Larraz, K. Siu, A. Moitra, J. Interrante, W. Smith, and et al. 2021. "VERDICT: A Language and Framework for Engineering Cyber Resilient and Safe System." *Systems.*

NCC Group. 2022. "ASCE 5.1 datasheet." *ASCE Software Overview.* Accessed Jan 16, 2024. https://www.adelard.com/media/gqcbmjxh/mk138v11_asce_51_datasheet.pdf.

—. 2024. *Defence.* Accessed Jan 16, 2024. https://www.adelard.com/sectors/defence/.

Netkachova, K., O. Netkachova, and R. Bloomfield. 2015. "Tool Support for assurance case building blocks." *SAFECOMP 2015.* Springer. 62-71.

Owre, S., and I. Mason. 2016. *Github - ETB.* Aug 19. Accessed Apr 20, 2023. https://github.com/SRI-CSL/ETB.

Perlroth, N., D. E. Sanger, and J. E. Barnes. 2021. "Widely Used Software Company May Be Entry Point for Huge U.S. Hacking." *The New York Times*, January 6.

rcm2 limited. 2014. *Integrated Safety Case Development ISCaDE Safety Requirements, Goals and Hazard Log All in One.* Accessed Jan 9, 2024. http://www.iscade.co.uk/.

Roback, K. P., D. A. Sparrow, and D. M. Tate. 2022. *A survey of current tools to develop and manage assurance cases.* P-33140, Alexandria, VA: Institute for Defense Analyses.

Woodham, K., M. Holloway, M. Barry, and R. Mays. 2012. *certware.* Accessed April 7, 2023. http://nasa.github.io/CertWare/.

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
01-2024	Document	START DATE	END DATE

4. TITLE AND SUBTITLE
Review of Potential Assurance Case Tool Options for DoD

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
HQ0034-19-D-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
AX-01-3100		

6. AUTHOR(S)
Roback, Kevin, P.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22305

8. PERFORMING ORGANIZATION REPORT NUMBER
D-33524 /2
H 2024-000007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Mr. Chris Collins Developmental Test, Evaluation, and Assessments (DTE&A)		

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The assurance case framework has the potential to improve the safety certification process for complex systems; however, effective implementation of it relies on tools to help one build a complex assurance case. We previously conducted a survey to identify available assurance case tools. We now build on this work by attempting to directly access assurance case tools and evaluate their ease of installation and use hands-on. Our work uncovered a litany of possible cybersecurity issues with assurance case tools, which make 16 of 17 open access tools studied in this work unsuitable for DoD use. We also contacted 6 commercial assurance case tool developers; though full trial versions of tools were not always available, we identified multiple commercial assurance case tools lacking obvious cyersecurity issues that may be suitable for DoD use. However, given the range of issues identified (and possibility of further unnoticed issues), it may be worthwhile for DoD to invest in assurance case tool development in-house, if DoD intends to push the assurance case approach. We also investigated linkages between assurance case tools and tools for model-based systems engineering (MBSE), and found that very few tools mentioned MBSE or linked to MBSE tools.

15. SUBJECT TERMS
Model-based System Engineering (MBSE); Assurance case; Cybersecurity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER
John Hong	703-845-2564

PREVIOUS EDITION IS OBSOLETE.

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

Distribution Statement A: Approved for public release; distribution is unlimited.