

Assurance Is an N-Space (Where N Is Hopefully Small)

Jeffrey Williams
williams@arca.va.com

Joel Sachs
sachs@arca.md.com

Douglas Landoll
landoll@arca.md.com

Diann Carpenter
carpenter@arca.md.com

Arca Systems, Inc.

8229 Boone Blvd., Suite 610
Vienna, VA 22182
(703) 734-5611

1. Introduction

Significant progress in the area of assurance cannot be made without recognizing its multi-dimensional nature. Our challenge is to create a vehicle for understanding and reasoning about assurance that supports its many dimensions. The creation of an assurance N-space provides a framework which supports many different aspects of assurance and, more importantly, the needs of its many consumers. This position paper describes such a space.¹

2. Assurance N-space

A simplistic view of assurance is that it is a degree of confidence about how something will perform relative to security. This confidence can be conveyed to others by means of evidence, which is produced by assessment processes such as TPEP. Figure 1 illustrates various examples of key ingredients that relate to assurance, such as the development of evidence and the establishment and consumption of confidence. Note there is a cyclic relationship, since confidence can become evidence to another consumer.

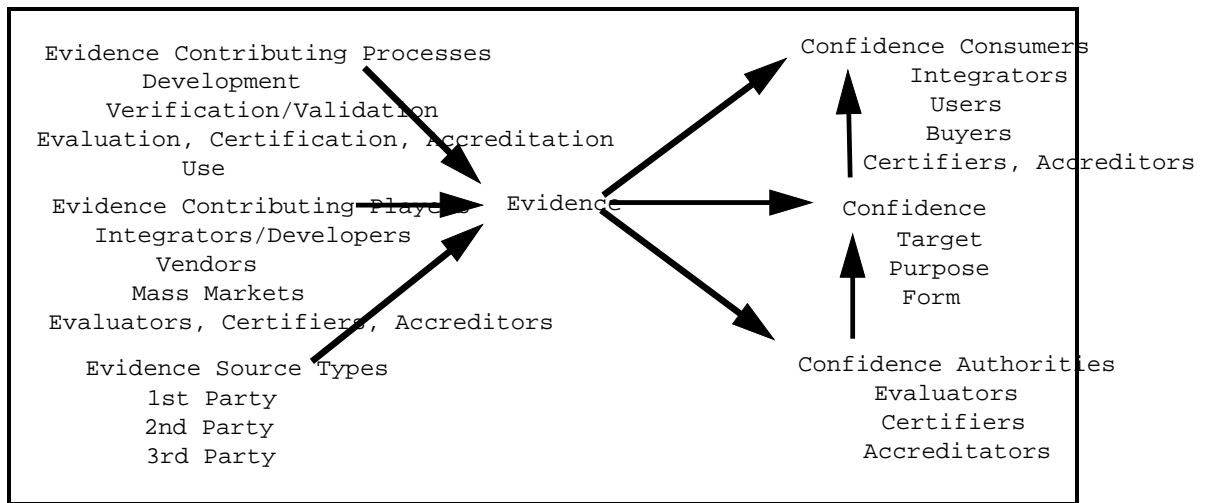


Figure 1: Example Ingredients to Establishing and Using Assurance.

Because the evidence produced by each activity differs, comparisons are often misdirected. Similarly, different types of assessment lead to different types and levels of confidence. A recognition of the many different dimensions of assurance is required. For example, a

¹ This work is supported by the National Security Agency under the SSEMS Contract MDA904-93-C-C029. The work is being accomplished as a joint effort by NSA and the Arca SSEMS Team.

comparison between the TPEP process under the authority of NSA and the same process run by private industry is not accurate unless it considers competency, objectivity, and authority of the evaluators (and there may be other factors). These influencing factors are some of the dimensions which define the assurance N-space.

3. Dimensions

The N-space view of assurance contains dimensions that help characterize many different types of assurance. Possible targets for this assurance include systems, products, mechanisms, processes, people, and companies. The dimensions shown in Figure 2 are examples of the various factors that affect the level of confidence in an assurance target.

Direct Dimensions	
Correctness	[level a.....level b.....level c.....level d]
Effectiveness	[low.....medium.....high very high]
Workmanship	[poor good fine excellent]
Others?	
Indirect Dimensions	
Process Maturity	[initial repeatable..... defined..... managed.....optimized]
Process Trustworthiness	[low.....medium.....high very high]
Environment Trustworthiness [level 1..... level 2 level 3..... level 4 level 5]
People Authority	[unrelated..... indirect..... direct]
People Trustworthiness	[low.....medium.....high very high]
People Competency	[novice experienced expert]
People Objectivity	[very biased biased..... unbiased]
Others?	
Discrete Dimensions	
Evidence Lifecycle Activity	[requirements, design, development, validation, verification...]
Evidence Producer	[developer, assessors, customer, user,]
Assurance Target	[system, product, mechanism, operation, process, people, companies]
Assessment Method	[first party, second party, third party]
Assurance User	[integrator, purchaser, user, ...]
Assurance Form	[rating, report, profile, credential, ...]
Others?	

Figure 2: Example dimensions for assurance demonstrate complexity.

The first set of dimensions are the “direct” dimensions. These dimensions describe a level of confidence in the assurance target itself. These dimensions are familiar and have been examined by TPEP, ITSEM, and other traditional assessment processes.

The second set of dimensions are the “indirect” dimensions. These dimensions are one step removed in that they examine evidence about the direct assurance. For example, performing background investigations on development personnel produces indirect evidence that the code is trustworthy. These indirect dimensions are not so familiar and have only recently been examined in the TSM.

The last set of dimensions are the “discrete” dimensions. These dimensions help to organize evidence into logical groups for evaluation purposes. Each of the direct and indirect dimensions

needs to be considered relative to each of the values of the discrete dimensions. For example, all the correctness evidence produced can be categorized by lifecycle phase, producer, target, etc...

4. Observations

This section discusses two important observations about the N-space view of assurance. The first deals with the “trade-offs” made in the design and development of systems. The second is that the N-space view can support multiple levels of understanding.

Equivalency Classes

The N-space view may facilitate the process of determining appropriate “trade-offs” of assurance evidence. Equivalency classes could be created to show which groupings of evidence will yield equivalent assurance. For example, if two sets of evidence establish the same degree of confidence in an assurance target and have the same purpose, then these sets can be considered equivalency classes.

One use for these equivalency classes is in determining a set of assurance requirements. Trade-offs made at this stage will yield the set of evidence that best suits a particular program. Equivalency classes are also useful during design and development stages, when specific assurance choices are being made. Here, trade-offs will reveal the lowest cost and fastest way to achieve the required assurance.

For example, a program may wish to cut costs by trading an expensive third-party assessment for an internal first-party assessment. Other trade-offs might exchange one piece of high level evidence for lower level evidence from several dimensions. The N-space provides a framework for evaluating these decisions.

Graduated Views

The security community has tried to simplify assurance to a single view. This approach is flawed because different consumers of assurance have different needs. For example, an executive manager may simply need to know that a system is highly trustworthy. Meanwhile, a middle manager needs some additional details, such as assurance sources and levels of direct and indirect assurance. Finally, technical people need to understand the assurance at a very detailed level.

Consider the different ways that we discover the nutritional value of a box of cereal. At one level, the front of the box prominently displays that the cereal is “Nutritional.” The concerned consumer may notice a smaller label that describes the cereal as “Low in Sodium, with Eight Essential Vitamins and Minerals.” For those experts who are very health conscious, the side of the box lists all the ingredients and percentages of the U.S. RDA contained.

Just as each of the different views of the nutritional information is important to a different type of consumer, the capability to provide different views of the same assurance information is critical to meeting the needs of the many different assurance consumers.

5. Conclusions

Viewing assurance as an N-space is a valuable way to deal with increasingly complex assurance sources, processes, and targets. In order to “solve” the assurance problem, the different

dimensions of the N-space need to be investigated, understood, promoted, and used both individually and collectively.

For the N-space view of assurance to be effective, N should be as small as possible. This can be achieved by reducing the dimensions to the minimum level that will still satisfy all consumers of assurance. On the other hand, because the N-space view can support different consumers at different levels of granularity, in particular collapsing views targeting executive, middle management, and engineering levels.

Further work needs to be done to facilitate the process of creating security confidence. First, the dimensions that are the most important to security need to be identified and refined. Methods for measuring each of these important dimensions should then be developed. Finally, equivalency classes should be explored to facilitate trade-offs between different types of assurance, first subjectively and then quantitatively.