Building a Case for Assurance from Process[1]

Karen Ferraiolo, Lisa Gallagher, Victoria Thompson
Arca Systems, Inc.
Phone: 703-734-5611
FAX: 703-790-0385
ferraiolo@arca.com
gallagher@arca.com
thompson@arca.com

Abstract

This paper reports on a project that involved research to determine the contribution of process capability to assurance and to define metrics for use in the development of process-based assurance arguments. The contribution of process capability, as measured by the Systems Security Engineering Capability Maturity Model (SSE-CMM), to assurance was studied. Recommendations were made for future work that would be needed to further the use of the SSE-CMM as a process-based assurance mechanism. The paper presents the objectives of the research, describes the work accomplished to support these objectives, and presents the results and recommendations from the research.

Keywords: assurance, process, process capability, capability maturity model, Systems Security Engineering Capability Maturity Model, SSE-CMM, certification, evaluation

1.0 Introduction

This paper reports on a project that involved research to determine the contribution of process capability to assurance and to define metrics for use in the development of process-based assurance arguments. The contribution of process capability, as measured by the Systems Security Engineering Capability Maturity Model (SSE-CMM), to assurance was studied. Recommendations were made for future work that would be needed to further the use of the SSE-CMM as a process-based assurance mechanism. Specific objectives of the research included answering the following questions:

- Would demonstration of process capability provide assurance?
- How can the contribution of process to assurance be measured?
- Can SSE-CMM profiles for specific types of organizations, products, and systems be formulated for the purpose of building assurance arguments?
- What kinds of tools are needed to facilitate the use of the SSE-CMM in building an assurance argument?

[1] This research was supported by the National Institute of Standards and Technology under Contract Number 50-DKNB-7-90099.

Section 2 of this paper describes the work accomplished to support these objectives. Section 3 presents the results and recommendations from the research. Section 4 summarizes conclusions from the work accomplished.

2.0 Work Completed

The work accomplished for this project included: 1) an analysis of current security evaluation/certification programs to determine what kinds of evidence provide assurance and how the SSE-CMM relates to the evaluation/certification requirements; 2) an analysis of security provider organizations to determine the relevance of the SSE-CMM to assurance activities performed by the organizations; 3) identification of ways to measure the contribution of process capability to assurance; and 4) development of assurance arguments based on the SSE-CMM.

2.1 Task 1: Analysis of current evaluation/certification programs

Task 1 involved analysis of current evaluation/certification programs with the objectives of: 1) determining what kinds of evidence provide assurance, and 2) determining how the SSE-CMM [SSE97] relates to evaluation/certification requirements. The detailed analyses of the Trusted Computer Systems Evaluation Criteria (TCSEC) [DOD85], the Common Criteria [CC96], and the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DOD97] are provided in [FER97].

2.2 Task 2: Survey of provider organizations

Task 2 included a survey of provider organizations with the objective of determining the relevance of the SSE-CMM to assurance activities performed by security engineering provider organizations. The questionnaire used to survey organizations was based on the Engineering Process Areas of the SSE-CMM and is described in Section 2.2.2. The results of surveying organizations to determine the relevance of the SSE-CMM to assurance activities is provided in [FER97] with a summary given in Section 2.2.3 of this paper.

2.2.1 SSE-CMM Workshop Survey Results

Before developing the provider organization survey, fifty-six responses to a survey that was distributed at the SSE-CMM 2nd Public Workshop in July 1997 were reviewed. . The Workshop survey asked for an indication of relative importance of the SSE-CMM Process Areas (PA). Only the PA names were used. Regardless of the type of their organization (e.g., Integration, Product Development, Evaluation, Manufacturing) most respondents indicated that all the SSE-CMM Engineering PAs were very important to their organizations, with the exception of the PAs relating to operations and maintenance. (Many respondents indicated that the operations and maintenance PAs were not at all important to their organization. There is reason to believe that the respondents were thinking in terms of end user operations and maintenance, as opposed to operation and maintenance of their own environments, which are also covered by these PAs.) Specific engineering PAs that were viewed as very important to the organizations include: Specify Security Needs; Provide Security Input; Verify and Validate Security; Assess Operational Security Risk; and Determine Security Vulnerabilities.

2.2.2 The Survey of Provider Organizations

The initial assumption before executing this survey was that performance of the SSE-CMM Engineering PAs provides some sort of assurance in the end-result. The survey for this research was developed using the Engineering PAs from the SSE-CMM. However, instead of using only the PA names, specific questions were formulated for each of the PAs based on the goals of the PAs. In the SSE-CMM, each PA has associated with it goals that indicate what is expected to be observed as a result of compliance with the activities defined in the PA. Additional questions were asked regarding metrics, the importance of security engineering activities, and the relationship between security engineering activities and the end results.

Interviewees were identified from various types of organizations: Service Provider; Integrator; Product Vendor; and Certifier/Evaluator. Interviewees were asked to answer the questions as the activities are performed in their own organization. They were also asked to indicate the confidence that performing that particular activity gave them in the security of the end result. Note that when the questions were asked of Certifier/Evaluator organizations the interviewee was asked to think about the activities that the Integrator/Vendor performed and to indicate the confidence in the end result that they received as a result of the Integrator/Vendor performing that activity.

2.2.3 Survey Responses

The results of the survey were fairly consistent across the different provider types. Table 1 lists the activities that the interviewees indicated were required most often. Table 2 lists the activities that were viewed as most likely to lead to project success. The interviewees were asked to indicate the assurance gained from the activity. This is also listed next to each activity.

Activity	Assurance Gained
risk assessment	environment is secure
requirements definition	requirements are complete/correct
accreditation documentation	customer knows what they're getting

Table 1. Activities Required Most Often

Activity	Assurance Gained
requirements definition/traceability	requirements are complete/correct
communication/ coordination	focus on important issues; building the right thing
risk analysis	environment is secure
security administration	reduced likelihood of malicious activities; current needs are being addressed

Table 2. Activities Most Likely to Lead to Project Success

2.2.4 Interviewer Observations

The following are observations made by the interviewers:

- Most interviewees had not thought about the assurance they were getting from performing security engineering activities until they had to answer for each of the questions. It seems they had felt that they were doing them simply because they were required (e.g., C2 product development, for certification purposes).
- Even those who were aware of the assurance gained stated that they probably wouldn't perform the activities if the customer weren't paying for it.
- Most indicated that security requirements definition/traceability and risk assessment were the most important activities and were most likely to lead to the success of the project. Many indicated coordination and communication were important.
- Vulnerability analysis seemed to be practiced in a very ad hoc manner, even by those organizations who were perceived to be mature. Product developers in particular focused on known rather than potential vulnerabilities.
- Almost none of the interviewees were aware of the activities involved in ensuring their own computing environment was secure.

2.3 Task 3: Methods for measuring process-based assurance

This task examined ways to measure the contribution of process to assurance. Two ways of measuring that contribution were considered: 1) the current SSE-CMM appraisal method and the results of application of the method, that is SSE-CMM Rating Profiles, and 2) the use of the assurance framework.[WIL98] These methods are described briefly in this section.

2.3.1 SSE-CMM Rating Profile

Figure 1 illustrates an example Rating Profile that would result from an SSE-CMM appraisal of an organization's process capability against specific PAs.Process capability is measured by five capability levels as defined in the SSE-CMM. The SSE-CMM Rating Profile illustrates the organization's capability level in any one or more of the PAs.

While it was initially anticipated that SSE-CMM Rating Profiles might be a way to measure assurance gained from use of the SSE-CMM, it became clear that the Rating Profile does not provide complete information with respect to assurance. That is, there are claims that could be made that the Rating Profile does not indicate.

It was also anticipated that Rating Profiles could be developed to provide guidance for different types of organizations and for different levels of assurance (i.e., according to the TCSEC for example). However, the analysis in Task 1 showed that although there is quite a bit of overlap between SSE-CMM activities and activities defined in the TCSEC, CC, and DITSCAP, there is not a one-to-one mapping. It would be difficult to claim that a specific SSE-CMM Rating Profile could satisfy requirements of a specific assurance level. In addition, considering the results of the survey in Task 2, all of the engineering PAs with the exception of PA04 (Attack Security) were either performed by the organization or the interviewee thought they should be performed. The fact that the activities were not consistently performed indicates that there is the need for some guidance with regard to security engineering activities. However, it is not clear that an SSE-CMM Rating Profile provides the level of granularity that is needed. Most interviewees indicated they hadn't realized the importance of the activity until they attempted to answer the question about assurance gained from performance of the activity.

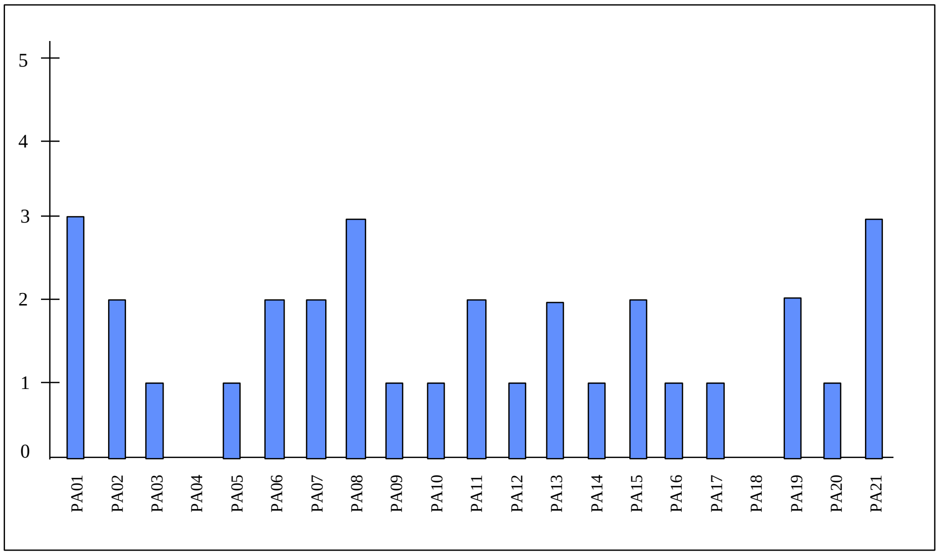


Figure 1. An SSE-CMM Rating Profile

2.3.2 Assurance Framework

An Assurance Framework [WIL98] has been developed to provide guidance on how assurance might be measured and communicated, how much assurance one needs, and how various types and sources of evidence relate. The framework defines assurance as "a measure of confidence in the accuracy of a risk measurement," taking into account that informed decisions about security depend on a complex set of factors related to both assurance and risk. The framework offers a way to build upon quantitative risk measurement methodologies and to employ them in such a way as to yield a rough measure of assurance that would permit one to trade off the relative merits of seeking more evidence to gain greater assurance against employing more safeguards to reduce risk.

The framework defines an Assurance Argument as a way of assembling evidential data in order to derive values for risk and assurance. There are four elements used in structuring an Assurance Argument:

Claims:	statements that something has a particular property
Evidence:	empirical data on which a judgment can be based
Reasoning:	statements which tie evidence together to establish a claim
Assumption Zone:	limit of an argument where claims are accepted without evidence

Assurance Arguments are sets of claims supported by evidence and bounded by a set of assumptions. These arguments are nested in the sense that each argument is composed of lower-level supporting arguments and evidence. The cycle of generating lower level claims and supporting evidence continues until it is reasonable to assume the claim without further evidence. This stopping point is called the assumption zone.

2.4 Task 4: Process-based assurance arguments

Task 4 was initially intended to postulate SSE-CMM Profiles for specific types of organizations, products, and systems for the purpose of building assurance arguments. It was anticipated that results of the previous tasks would indicate that process capability in certain areas would make valuable contribution to assurance in specific areas. While both Task 1 and 2 support this, as noted in the discussion of SSE-CMM Rating Profiles for Task 3 above, it became clear that an SSE-CMM Rating Profile does not provide the correct mechanism to measure or illustrate this contribution. What has become clear is that there is the need for guidance in using the SSE-CMM and in understanding the value of using the SSE-CMM to develop an assurance argument or product assurance evidence. Rather than focus on the development of SSE-CMM profiles, this task then, focused on the feasibility of developing assurance arguments for use of the SSE-CMM in the following scenarios:

- Product vendor providing a TCSEC Level C2 product; and
- System certification following the DITSCAP.

The results of this task are presented in [FER97] and discussed in Section 3.3.1.

3.0 Results

The results of the research are presented in this section by answering the stated objectives of the project.

3.1 Objective 1: Contribution of process capability provide assurance

The results of the work accomplished convince us that the demonstration of process capability can contribute significantly to assurance. In Task 1, in which we analyzed the TCSEC, TPEP process, Guidance for applying the TCSEC in Specific Environments, Common Criteria Assurance Requirements, and the DITSCAP, we learned that the process areas defined in the SSE-CMM correspond well with the processes of these traditional assurance methods. Our Task 2 research into the processes on which various types of organizations rely for assurance revealed that all of the processes defined in the SSE-CMM are considered to contribute to the development of assurance arguments by integrators, product developers, evaluators and manufacturers alike. And as part of our Task 3 efforts, we were able to perform an initial detailed mapping of the SSE-CMM to the TCSEC C2 criteria and to the DITSCAP, which demonstrates that, with appropriate guidance, tailoring, and evidence gathering, results of an SSE-CMM assessment can support or even replace important aspects of traditional assurance methods.

As a result, we now view process capability, as measured by the SSE-CMM, as a "common thread" that logically links other traditional assurance methods. While it is difficult to relate assurance that results from formal product evaluation against the TCSEC or the Common Criteria, to assurance that results from applying the DITSCAP, the SSE-CMM can be used to guide or contribute to development of these and other forms of assurance. The development of guidance for using the SSE-CMM as described in Section 3.4 will be of tremendous value to secure product and system developers and integrators, security service providers, product evaluators and assessors, system certifiers and accreditors, acquirers of products and systems, and other initiatives (e.g., the Common Criteria Project, TPEP, and Trusted Technology Assessment Program (TTAP)) interested in alternative assurance techniques. We see that this would be especially valuable in complex programs, such as integration efforts, in which assurance arguments must be developed for individual components as well as a system overall.

3.2 Objective 2: Measuring Process Assurance

Tasks 1 and 2 provided an understanding of how the SSE-CMM contributes to current assurance criteria as well as how various providers and consumers of assurance view the contribution of process to assurance. These tasks indicate that process capability can be measured by determining:

- the existence of evidence and artifacts, (an indicator of compliance with and execution of relevant base practices), and
- the maturity of processes (as measured by the SSE-CMM Generic Practices[GPs]).

In Task 2 interviewees were asked about metrics with regard to security, but results indicated very few collected any data. Organizations that were perceived to be more mature in their processes (though not necessarily security engineering processes) gave examples of metrics they collected: software defects; failed tests; requirements changes. Relating these examples to the security engineering discipline and considering artifacts that are important to those interviewed, we have postulated metrics that should be collected in order to track the success of security engineering efforts. These include:

- system/product vulnerabilities,
- deviations from policy,
- cost deviation,
- schedule deviation,
- number of policy changes,
- number of security requirements changes,
- use of security features,
- failed security tests,
- success of system accreditation effort, and
- success of product evaluation effort.

The correlation between process capability and, for example, the success of an evaluation or certification effort, as measured using these data points would provide a measure of the contribution of process capability and assurance.

3.3 Objective 3: Using Process Capability to Build Assurance Arguments

As reported for Task 2, our research has shown that the creation of profiles (whereby the relevant PAs are specified, as well as the appropriate capability level required for each PA) by specific types of organizations, products, and/or systems may not be very useful for the purpose of building assurance arguments (see Observations in this section). Specifically, the research shows:

- there is quite a bit of overlap between SSE-CMM activities and activities found in the TCSEC, the DITSCAP, and the CC (Task 1),
- most organizations surveyed are performing all or most of the activities (or think they should be performed) regardless of any assurance requirement to perform them (Task 2),
- there was a clear indication that an SSE-CMM Rating Profile does not provides the level of granularity that is needed. Although there is a relationship between the SSE-CMM activities

and assurance methods as discussed above, there is not a direct, one-to-one mapping. Therefore, requiring a specific SSE-CMM Rating Profile would not provide enough information for either the provider or consumer of the assurance/evidence provided by performance of SSE-CMM activities (Task 2),

- while use of the SSE-CMM *can* contribute to assurance, there is the need for guidance in using the SSE-CMM, and in understanding the value of using the SSE-CMM to develop an assurance argument or product/system assurance evidence (Task 2).

3.3.1 Assurance Arguments

Rather than focus on the development of SSE-CMM profiles then, Task 4 focused on the feasibility of developing assurance arguments and providing assurance evidence from an SSE-CMM appraisal. Using the recently updated Assurance Framework [WIL98] described in Section 2.3 of this report, an assurance argument was developed for the example cases of:

- A product vendor providing a TCSEC Level C2 product; and
- A system certification following the DITSCAP.

Detailed mappings are provided in [FER97]. For these example cases, a top level claim was developed. This top level claim is the root of the assurance argument. All lower level claims, evidence and reasoning go towards establishing this claim. Lower level supporting claims were developed, and sometimes organized according to the categories: People, Process, Environment, and Technology. People includes anyone who may affect the security of the enterprise, system or product. Process consists of any activities that establish, affect, or maintain the security of the enterprise, system or product. Environment may include location, physical setting, or organizations culture, etc. Technology refers to the combination of hardware, software and communications that automate the processes of the enterprise, system or product. Lower level claims were refined and specific SSE-CMM evidence was presented to directly support a claim.

Of course, when developing a complete assurance argument a vendor or developer would also offer additional evidence unrelated to the SSE-CMM. No attempt was made to presume what that evidence might be, as the objective was to show demonstrate the feasibility of mapping the evidence from an SSE-CMM appraisal to the claims being made about the product or system.

3.3.2 Observations

While developing these example assurance arguments, the research showed that the SSE-CMM appraisal results do directly apply to the claims being made. In the case of the DITSCAP, virtually all of the SSE-CMM PAs, as well as many of the GPs, could be offered as evidence. In the case of the C2 argument, some of the PAs were directly applicable. This appears to be dependent on the type and nature of the assurance requirements and the resultant claims being made. The DITSCAP requirements, for example, are largely related to the certification *process*, and thus the SSE-CMM is largely applicable. With regard to process capability as measured by the SSE-CMM GPs, it was found in both the C2 and DITSCAP that a particular Capability Level was not apparent. For example, not all of the GPs for Level 2 were applicable in either case. Further, for the DITSCAP, some Level 3 GPs were applicable.

Considering the applicability of the SSE-CMM evidence as demonstrated by the example mappings to the C2 requirements and the DITSCAP, the following observations are made regarding the benefits of the SSE-CMM for assurance:

- For the evaluators (e.g., NSA, commercial TEFs) and certifiers, the SSE-CMM can provide direct evidence regarding process claims, as well as a uniform manner to evaluate of claims and evidence, thus contributing to the normalization of the evaluation/certification process - making the process more defined and repeatable, and less intuitive. Ultimately, this direct benefit can be measured in terms of cost/schedule savings to evaluation and certification efforts.
- For the product vendor or system developer, direct benefits include a cost savings in the evaluation (evaluation discount) or C&A cost/schedule savings, based on the savings incurred by the TEF or certifier as mentioned above, and,
- For the product vendor or system developer, the SSE-CMM offers an organization a method of gaining and measuring assurance that is applicable to various types of assurance arguments, and provides a practical, economical, and reusable way to enhance their ability to meet various assurance requirements.

It is also clear that it would be beneficial to begin to gather some of the data suggested in Objective 2 above by performing an example appraisal for a developer or vendor involved with the evaluation or certification process. The relationship to the process maturity of the organization assessed to the ultimate success of the evaluation/certification effort could be determined using the measures suggested above.

3.4 Objective 4: Tools to Facilitate the use of the SSE-CMM in Building an Assurance Argument

All of the tasks indicated the need for various types of tools that might be useful in building a process capability-based assurance argument. The following were identified:

- *Guidance for interpreting the SSE-CMM PAs in different contexts.* For example, the operations and maintenance PAs can be applied to the operation of a developed system or to the development environment of a product or system being developed.
- *Training in how to use the SSE-CMM.* During the survey it became apparent that many organizations were not practicing security engineering in a way that ensured security issues were being addressed and communicated/coordinated across their projects.
- *Guidance in developing assurance arguments and gathering evidence using the SSE-CMM.* This guidance would need to be developed to support various users from certifiers/evaluators and end user/customers to gain assurance that their security needs have been met to integrators/vendors who want to show they are capable of producing secure systems and products.
- *Guidance for appraisers for performing appraisals when the results will be used to support specific claims.* This guidance should include such items as appraiser/appraisal team qualification requirements (e.g., knowledge of evaluation process), lists of specific evidence or artifacts applicable to certain claims, and requirements for the specific quality of the evidence. An associated tailorable automated Data Tracking Sheet could be developed for use during each type of appraisal that facilitates evidence gathering and evaluation, and score generation.
- *Guidance for both developers and consumers of assurance arguments on how to use the SSE-CMM in developing or evaluating an Assurance Argument.*

4.0 Conclusions

As a result of this research we believe it is technically feasible to develop the guidance and training described in Section 3.4 and that such tools would be of tremendous value to:

- product and systems engineering organizations who must provide assurance to consumers;
- organizations who seek assurance in the products or systems they acquire;
- security evaluators, such as system certifiers and accreditors, product evaluators, and product assessors; and
- other initiatives, such as the AAWG, CC, Network Rating Model, Trusted Product Evaluation Program (TPEP) and Trusted Technology Assessment Program (TTAP), interested in alternative assurance methods.

5.0 References

[CC96] Common Criteria Project, “Common Criteria for Information Technology Security Evaluation, V1.0,” January 31, 1996.

[DOD85] Department of Defense, “Department of Defense Trusted Computer System Evaluation Criteria,” DoD 5200.28-STD, December 1985.

[DOD97] Department of Defense, “Department of Defense Information Technology Security Certification and Accreditation Process,” 1997.

[FER97] Ferraiolo, Karen; Gallagher, Lisa; Thompson, Victoria, “Final Report: Process-Based Assurance Product Suite,” December 23, 1997.

[SSE97] SSE-CMM Project, “Systems Security Engineering Capability Maturity Model, Model Description, V1.1,” June 16, 1997.

[WIL98] Williams, Jeffrey; Jelen, George, “A Framework for Reasoning about Assurance,” April 23, 1998.

Building a Case for Assurance from Process

Presented by:

Lisa A. Gallagher

Arca Systems, Inc.

gallagher@arca.com

(410)309-1780

Significance of the Problem

- **licensed TEFs**
- **DITSCAP implementation**
- **CC**
- **increase in security consciousness**
- **desire for assurance**
- **growing SSE-CMM market**

Need thread to tie together - need alternative assurance sources

Research Objectives

Determine:

- **Whether demonstration of process capability can provide assurance**
- **How the contribution of process capability to assurance be measured**
- **Whether process capability be used to build assurance arguments**
- **What kinds of tools are need to facilitate the use of the SSE-CMM in building an assurance argument**

Note: This work was performed by Arca through a SBIR project with NIST (Contract No. 50-DKNB-90099)

SSE-CMM Workshop Survey

- **Relevance of SSE-CMM process areas:**
  - **all are important**
  - **engineering process areas are very important:**
    - **specify security needs**
    - **provide security input**
    - **verify and validate security**
    - **assess operational security risk**
    - **determine security vulnerabilities**

SSE-CMM: Systems Security Engineering Capability Maturity Model

Follow-up Phone Survey

- **Organizations surveyed:**
  - **service providers**
  - **integrators**
  - **product vendors**
  - **certifiers/evaluators**
- **Data collected:**
  - **types of activities performed**
  - **assurance gained from performance of the activity**
  - **importance of the activities**

Follow-up Phone Survey Results

activities required most often

risk assessment → environment is secure

requirements definition → requirements are complete/correct

accreditation documentation → customer knows what they're getting

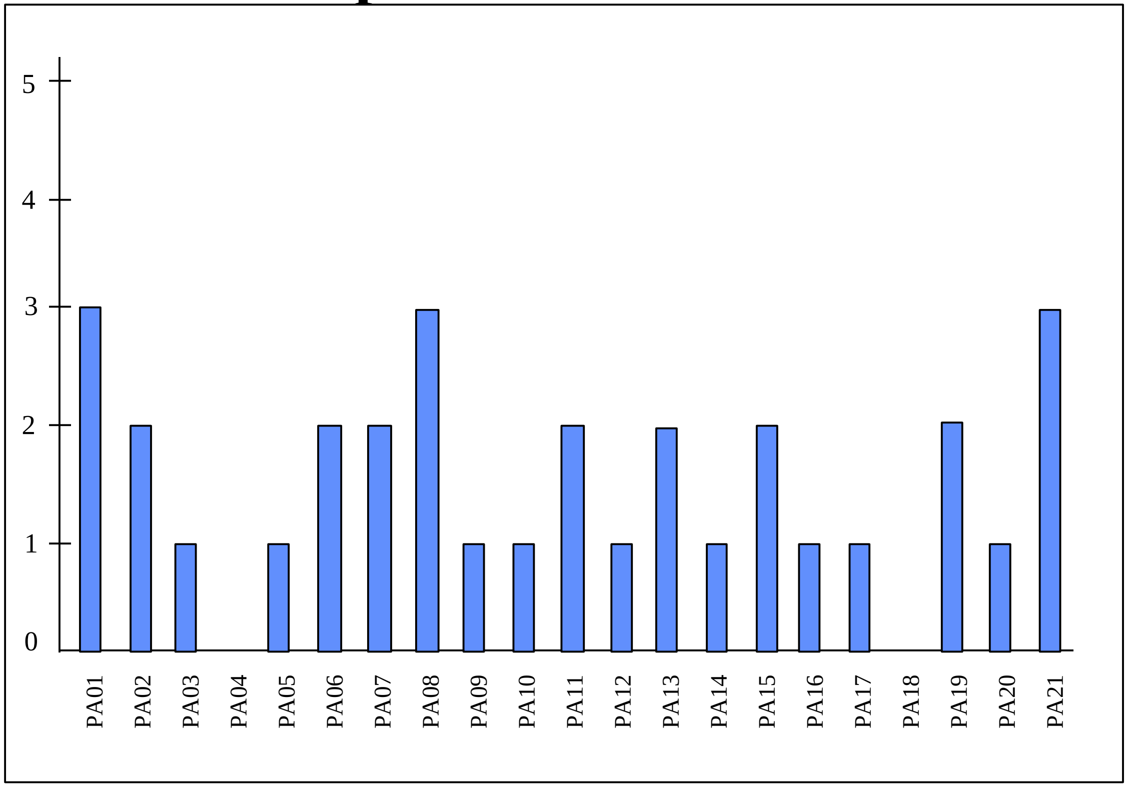
Follow-up Phone Survey Results (cont.)

activities most likely to lead to project success

requirements definition/traceability	→	**requirements are complete/correct**
communication/ coordination	→	**focus on important issues; building the right thing**
risk analysis	→	**environment is secure**
security administration	→	**reduced likelihood of malicious activities; current needs are being addressed**

Methods to Measure Process-based Assurance

Example SSE-CMM Profile



Issues include:

- **All SSE-CMM activities seen as important**
- **Overlap between SSE-CMM activities and assurance requirements**
- **Need more detailed(granular) information**
- **Need guidance in using the SSE-CMM for process assurance**

Using Process Capability to Build an Assurance Argument

- Developing an Assurance Argument
  - uses “A Framework for Reasoning about Assurance”*
- Results
  - guidance on where SSE-CMM provides assurance
  - mechanism for evaluators/certifiers to use in scoping their efforts and making tradeoffs

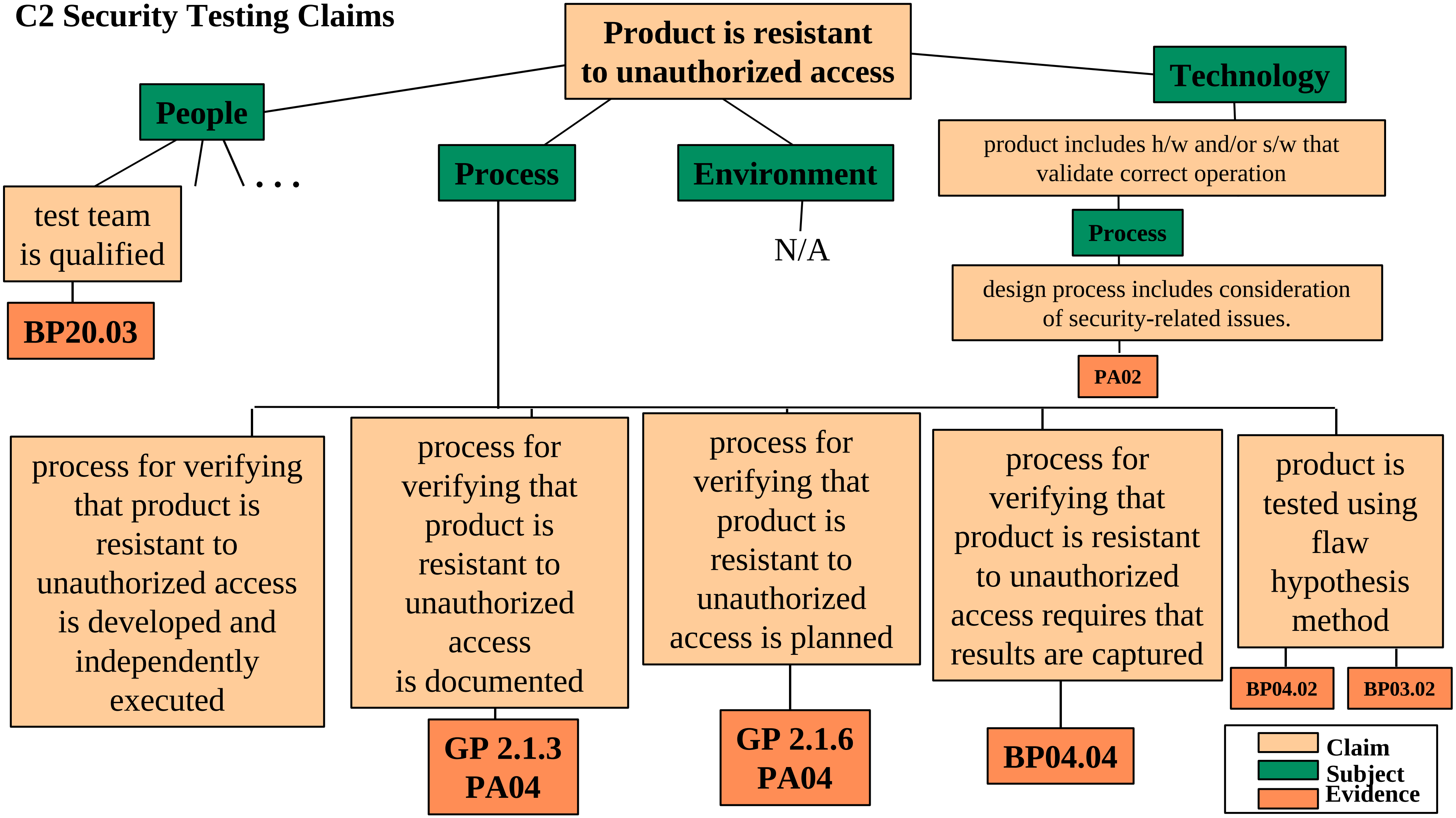
* This framework was developed by Arca under NSA Contract No. MDA904-97-C-0223

Elements of an Assurance Argument

- **Claims**
  - statements that something has particular properties
- **Evidence**
  - empirical data on which a judgment can be based
- **Reasoning**
  - statements which tie evidence together to establish a claim
- **Assumption Zone**
  - limit of an argument where claims are accepted without evidence

Example

C2 Security Testing Claims



Product is resistant to unauthorized access

People

test team is qualified

BP20.03

. . .

Process

Environment

N/A

Technology

product includes h/w and/or s/w that validate correct operation

Process

design process includes consideration of security-related issues.

PA02

process for verifying that product is resistant to unauthorized access is developed and independently executed

process for verifying that product is resistant to unauthorized access is documented

GP 2.1.3 PA04

process for verifying that product is resistant to unauthorized access is planned

GP 2.1.6 PA04

process for verifying that product is resistant to unauthorized access requires that results are captured

BP04.04

product is tested using flaw hypothesis method

BP04.02

BP03.02

🟧 Claim
🟩 Subject
🟥 Evidence

Benefits Identified

For evaluators/certifiers:

- **SSE-CMM appraisal results provide direct evidence regarding process claims**
- **use of SSE-CMM evidence can provide a uniform manner to evaluate claims and evidence, thus contributing to the normalization of the evaluation/certification process**

Benefits Identified (cont.)

For the product vendor/system developer:

- **Offers a method of gaining and measuring assurance that is applicable to various types of assurance arguments**
- **Offers a practical, economical, and reusable way to enhance their ability to meet a variety of assurance requirements**
- **May offer a cost/schedule savings based on that realized by the evaluator/certifier**

Recommendations

Benefits to the community may be realized by making available:

- **Method for for using SSE-CMM to develop assurance arguments and enhance currently accepted certification and evaluation processes.**
- **Training**
- **Guidance**
- **Services**

Future Work - Continue Research

Objectives:

- **Document contribution of process capability to assurance**
- **Develop method for using SSE-CMM to develop assurance arguments and enhance currently accepted certification and evaluation processes**
- **Identify mechanisms to enable & deliver the method**
- **Lay groundwork for institutionalization of method and tools**

Future Work -
Continued Research (cont.)

Detailed Task Plan:

- **Complete example mappings of SSE-CMM to TCSEC C2 and B1, the DITSCAP, and to the CC**
- **Obtain review of mapping by authoritative bodies/individuals**
- **Develop mechanism to correlate process capability with certification/evaluation success, based on metrics identified in initial research (to support institutionalization)**
- **Develop specs for tools: training specification, services description, and draft guidance, develop/tailor SSE-CMM appraisal tools to support method**
- **Develop detailed institutionalization/commercialization strategy**

Future Work -
Deliver to Community

- Provide a commercially available method for using the SSE-CMM to build assurance arguments for the purposes of both evaluation and certification
- Communicate benefits to community
- Analyze impact on DITSCAP, TTAP, etc.
  - Pilots
- Pursue institutionalization of method:
  - Tie to Govt. org. mission, OSD strategic plan
  - Determine what policies/regs need to be in place
  - Influence policy makers and potential users

Long Term Benefits

The availability of the method will:

- **“stimulate" the SSE-CMM market (i.e., encourage use of the model)**
- **provide an extremely valuable (especially to the Government) assurance methodology**
- **“stimulate” the TTAP, CC and DITSCAP “markets” and make eval/cert better, cheaper, and faster, resulting in more available evaluated products and certified systems**
- **Arca will offer this as an SSE-CMM "Qualified Partner"/Consortium Member**