NASA

TASC

INSIGHT APPLIED™

KEYLOGIC

Annual NASA IV&V Workshop

Presented by Patrick Olguin
September 10, 2014

There and Back Again – Connecting Assurance Statements to Analysis Spreadsheets in Support of Evidence Based Assurance for the Ground Systems Development & Operations Program

Today's Goals

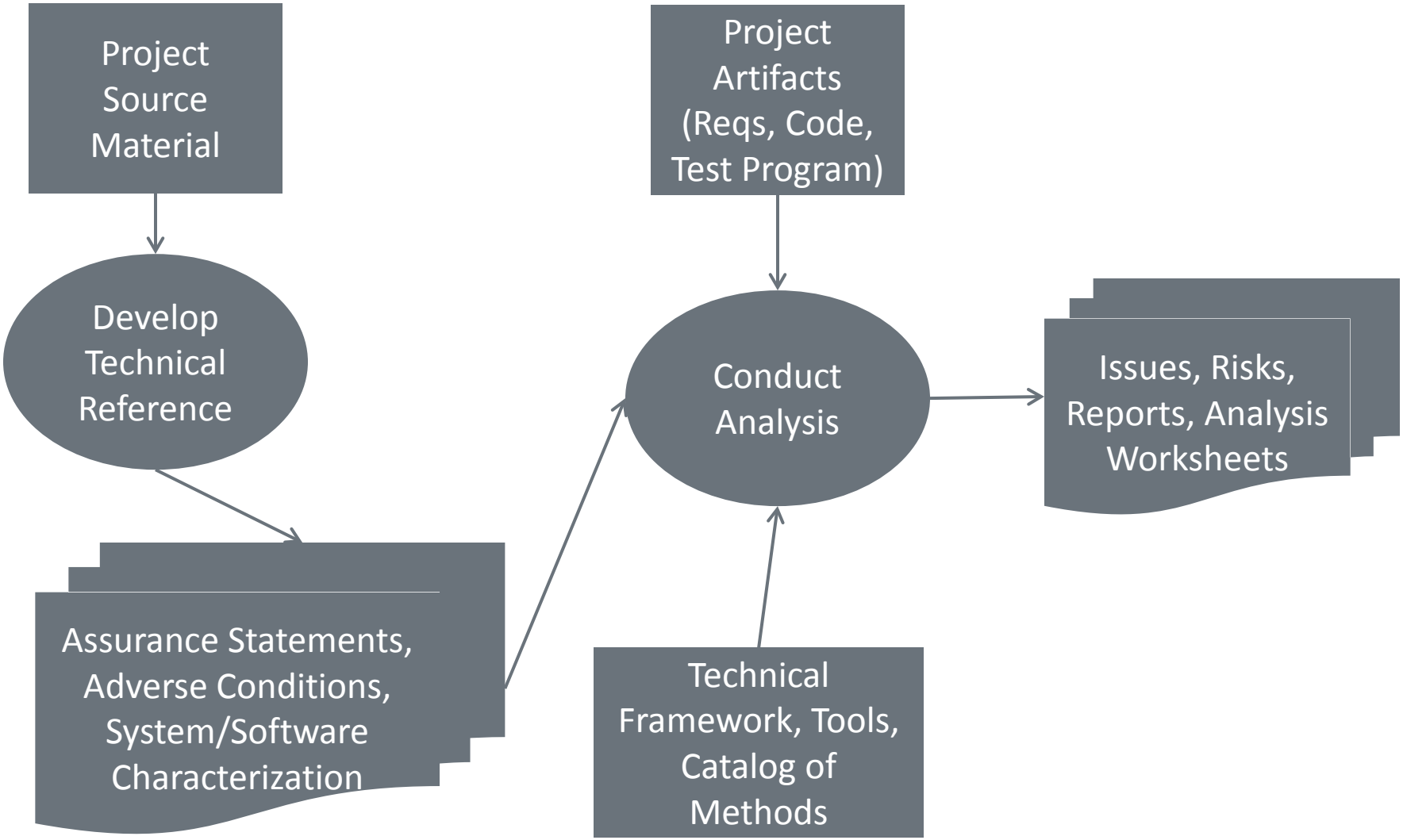
- Understand The Problem
  - The collision of customer requirements, management's goals, and the harsh reality of analyst's daily grind
- Stimulate discussion
  - This activity was really a proof of concept, and the current result is "one man's vision reviewed by a few others."
  - Path forward to a published approach
  - Hopefully find happy ground between shock/disbelief, enlightenment, relief and more focused technique
- Recognize that IV&V, like the projects we assess, requires two-way traceability in our artifacts to support our claims of assurance

Where We Want To Go

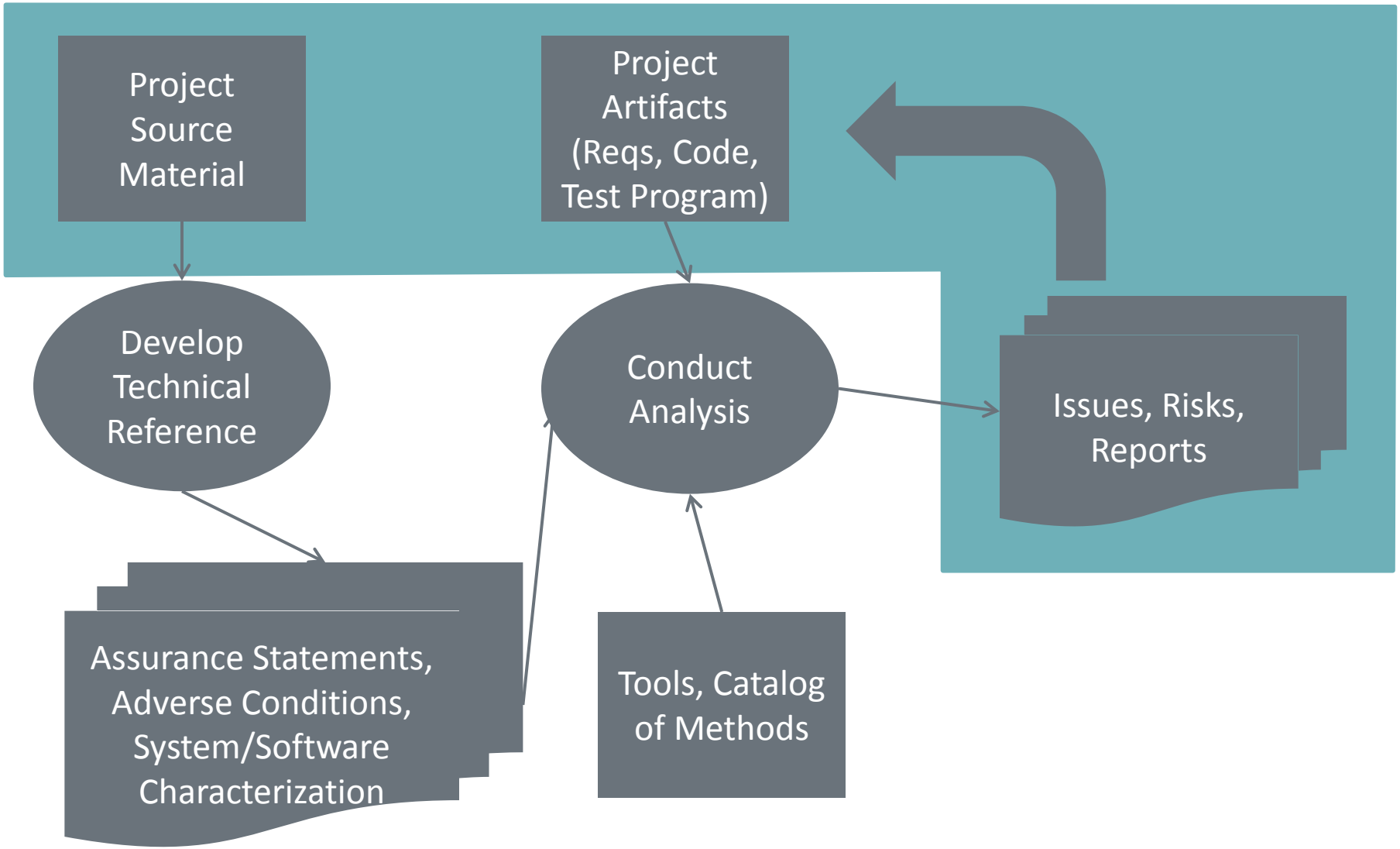
- Evidence Based Assurance demands* that IV&V analysis be quantifiable.
  - Accurately characterize the assurance provided – the magic metric IV&V has always sought
    - What is the value added?
  - Objectively assess residual risk
  - Support milestone reviews with metrics other than rack/stack of issues/risks
- How?
  - Scope, Tools, Catalog of Methods
- With What?
  - Technical Reference
  - "**IV&V Technical Reference is the collection of data and knowledge regarding IV&V's independent understanding of the system's software.** The Technical Reference serves as the basis for IV&V analysis. This information includes but is not limited to **system goals and needs, software interactions amongst system design elements, normal and abnormal behaviors and conditions of the system's software and the operational environment**.
  - "Serves as "objective evidence to either confirm or deny that the software artifacts are correct and complete"

*or at least strongly suggests

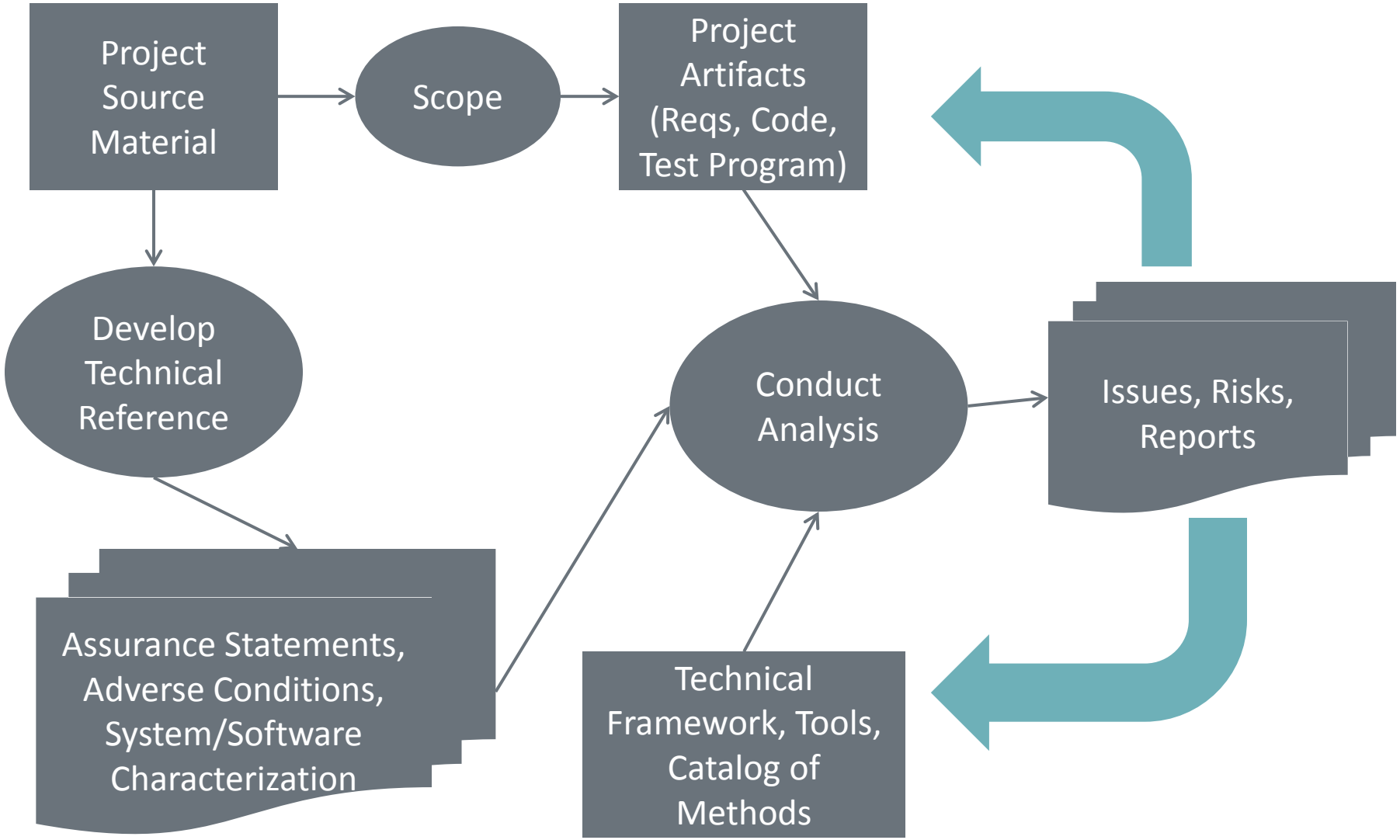
Evidenced Based IV&V Analysis – Overview



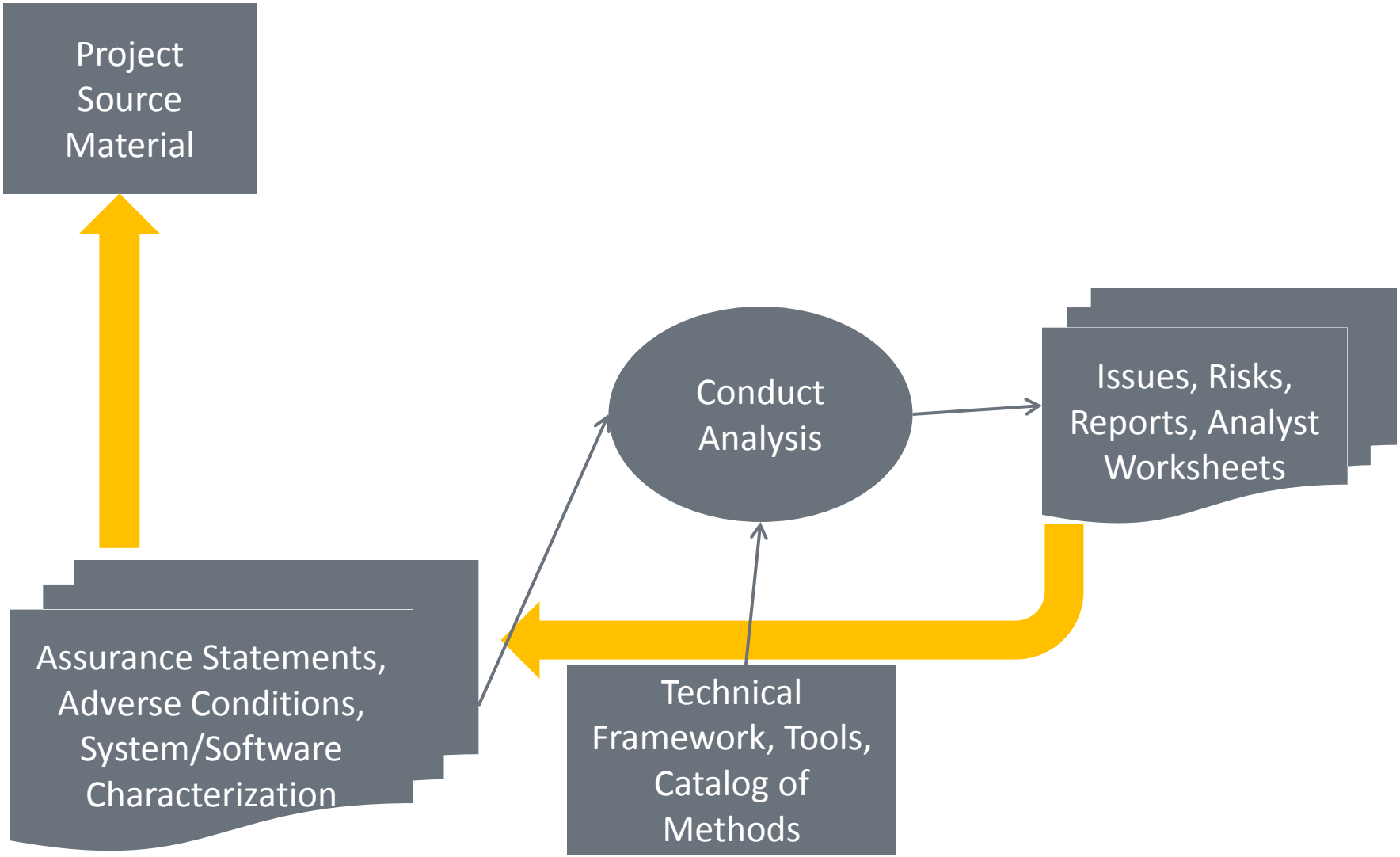
Evidenced Based IV&V Analysis – Project Perspective



Evidenced Based IV&V Analysis – Analyst Perspective



Evidenced Based IV&V Analysis – Problem



The Problem

- No path to directly relate analyst's daily work, and results backward
  - Assurance Cases
    - Therefore, can't answer the question – What level of assurance are you providing?
  - Adverse Conditions
    - Our understanding of the system software's preventive and responsive behaviors
    - Missing behaviors
  - Software and System Characterizations
    - Our understanding of the architecture of these system components
  - Project's High-level systems
    - Difficulty expressing impact to assurance in the "project's language"
- Difficulty quantifying residual risk resulting from
  - Limitations
    - Again – no trace through the reference material to project's high-level systems
  - Missing artifacts
    - Unable to characterize risk at systems level, when low-level artifacts are missing, late, immature.

Hypothesis

- If direct relationships between Assurance Claims/Statements, and current IV&V analyses/results can be established, and integrated directly into the analysts' spreadsheets, a quantifiable measure of assurance/risk for those claims can be derived from the analysts' spreadsheet-based analysis, directly supporting evidence based assurance.

The Next Problem(s)

- Assurance Statements don't just happen
  - Not every engineer is a free-thinking stream-of-consciousness philosopher who can pull this stuff out of thin air.
    - As a matter of fact, most of them aren't
  - Assurance Statements start looking like a functional decomposition, aka requirements, if you're not careful
  - The quality, quantity, availability, and applicability of reference material (high-level specs) varies widely
  - Tends to end up as a fill-this-square exercise, never to be considered again

The Next Hypothesis

- If analysts can be provided concrete examples of how to write assurance statements from their own project, and this material can be integrated into their daily work, we will have improved their ability to provide evidence of their assurance work

Anticipated Benefits

- Assurance Statements become a living document, instead of something developed and set aside
- The usefulness of this part of the Technical Reference becomes self-evident, as it is incorporated directly into the analyst's worksheets
- Assurance statements with consistent look, level-of-detail, and single "voice"
- Low-level results able to be rolled-up into high-level assurance statement summaries
  - Quantify the level of assurance provided,
  - Quantify current/residual risk stemming from gaps-in-assurance resulting from missing/delayed artifacts, schedule delays, and scope of IV&V analysis.
    - This is crucial, and the #1 complaint from analysts – we can't assure what we don't have (artifacts!)

Methods

- Developed top-level system claims from top-level project source material
- Decomposed high-level claims to assurance statements compatible with the level of detail of analysis spreadsheets
- Incorporated Adverse Conditions into the low-level assurance statements
- Created a several new pages for the analysts that dovetailed into their spreadsheet schema without blowing it up into an unmanageable 8-D
- Created mapping between assurance statements and project's software requirements (Project requirement number became the major key of the schema).
- Created a user's guide with examples, to help analysts develop assurance statements from reference material
- Analysts populated spreadsheets.
- Incomplete/delayed analysis was easily identified by empty cells in spreadsheets.

Ground Systems Development & Operations (GSDO) Program

Modern Spaceport

Vehicle Integration and Test

- Modernization of Vehicle Assembly Building (VAB)
- New Mobile Launcher
- Many legacy systems being upgraded.
- Local and Remote Control of GSDO hardware end items (Cryo Systems, Leak Detection, Range Safety, Power, Emergency Safing System, etc.)
- Display Software mirrors Programmable Logic Controllers (PLCs)
- IV&V focus is on software behavior of local and remote displays, during test and launch operations

"IV&V does what we can't"

First Steps – Actual excerpt from early Assurance Statement

1. Leak Detection Systems Remote and Display Software will operate safely when performing launch pad operations, under nominal and known adverse conditions.

1.1 Power-up Leak Detection System (LDS)

a) The LDS Local, Remote and Display software will operate safely when performing Power-up under nominal conditions.

b) The LDS Local, Remote and Display software will operate safely when performing Power-up LDS under known adverse conditions.

1.2 Power-down LDS

a) LDS Local, Remote and Display software will operate safely when performing Power-down LDS under nominal conditions.

b) LDS Local, Remote and Display software will operate safely when performing Power-down LDS under known adverse conditions, or the risks are known.

First Steps – Problems

- Top-level claim doesn't trace back to higher-level system claim
  - Difficult to express in project's language
- Doesn't address test/check-out scenarios
- Boiler plate statements don't add any value as reference material
  - Not enough detail to support requirements, design or code analysis
- Microsoft Word paragraphs not easily referenced from other documents/artifacts
  - No two-way tracing
- Not compatible with analysis worksheets used daily by analysts
  - The worksheets are critical not only to track issues but to quantify "goodness" of artifacts
- Essentially a square-filler exercise to satisfy compliance in developing technical reference.
  - Put away and forgotten

The New Approach – Assurance Statements as a Resource/Reference

- Let's build another spreadsheet!
- Features
  - Serves as a central repository/historical record of how the Assurance Statements were developed for the subsystem
  - Traces back to source material , with clickable link to the physical document used - in this case, Concept of Operations
  - Provides handy reference from IV&V project's Technical Scope and Rigor document for the subsystem
    - Scope of the work is built-in, ensuring the elaboration of the subsystem is consistent with the scope of the analysis
  - Hyperlink to requirements document under review
  - Links forward to applicable requirements document section
  - Basically – a dashboard, only a useful one!
- Development of the Assurance Statements also serves to increase overall understanding of system, enabling us to better speak to system-wide impacts from issues/risks discovered during analysis

The New Approach – Continued

	A	B	E	F	G
1	Top-level Claim				
2	The Ground Main Propulsion System software will monitor and control propellent and fluid commodities for the Space Launch System in response to automated and manual commands, safely as desired; preventively and responsively to adverse conditions, during initial integration and checkout, and during launch operations.				

Straight from Con-Ops

		Requirements					Test												
		3.1	3.2	3.3	3.4	3.5	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1
		Y	X	X	X	P	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X
3	TS&R																		

4	Supporting Statements	S/W ?	Scope Rationale	ConOps Ref	Original Text (optional)	Pro Cor
11	Perform Functional Verification	y	Command processing, display indicators	Sec 1.1	XXXXXXXXXXXXXXX	
12	Perform Cryos Electrical Checkout	y	Software used to display readings/indicators	Sec 1.1	XXXXXXXXXXXXXXX	
13	Perform HazGas Leak Detection	y	Uses HGDS system w/software	Sec 1.1	XXXXXXXXXXXXXXX	
18	Perform Pneumatic Checks	y	Software used to control valves, monitor status	Sec 1.1	XXXXXXXXXXXXXXX	

GMPS Assurance Stmts

The New Approach – Continued

	A	B	E	F	G
1	Top-level Claim				
2	The Ground Main Propulsion System software will monitor and control propellent and fluid commodities for the Space Launch System in response to automated and manual commands, safely as desired; preventively and responsively to adverse conditions, during initial integration and checkout, and during launch operations.				
3	TS&R				
4	Supporting Statements	?	Scope Rationale	ConOps Ref	Original Text (optional)
11	Perform Functional Verification	y	Command processing, display indicators	Sec 1.1	XXXXXXXXXXXXXXX
12	Perform Cryos Electrical Checkout	y	Software used to display readings/indicators	Sec 1.1	XXXXXXXXXXXXXXX
13	Perform HazGas Leak Detection	y	Uses HGDS system w/software	Sec 1.1	XXXXXXXXXXXXXXX
18	Perform Pneumatic Checks	y	Software used to control valves, monitor status	Sec 1.1	XXXXXXXXXXXXXXX

Requirements					Test												
3.1	3.2	3.3	3.4	3.5	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1
							TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X

One click gets you
To the Technical Scope
and Rigor Report

GMPS Assurance Stmts

The New Approach – Continued

	A	B	E	F	G
1	Top-level Claim				
2	The Ground Main Propulsion System software will monitor and control propellent and fluid commodities for the Space Launch System in response to automated and manual commands, safely as desired; preventively and responsively to adverse conditions, during initial integration and checkout, and during launch operations.				
3	TS&R				
4	Supporting Statements	S/W ?	Scope Rati	ConOps	al Text (optional)
11	Perform Functional Verification	y	Command display ind		XXXXXXXXXXXX
12	Perform Cryos Electrical Checkout	y	Software u readings/ir		XXXXXXXXXXXX
13	Perform HazGas Leak Detection	y	Uses HGDS system w/software	Sec 1.1	XXXXXXXXXXXXXXX
18	Perform Pneumatic Checks	y	Software used to control valves, monitor status	Sec 1.1	XXXXXXXXXXXXXXX

Requirements					Test												
3.1	3.2	3.3	3.4	3.5	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1
Y	X	X	X	P	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X

GMPS Assurance Stmts

Snapshot of the Technical Framework Elements in scope for this subsystem

The New Approach – Continued

	A	B	E	F	G
1	**Top-level Claim**				
2	**The Ground Main Propulsion System software will monitor and control propellent and fluid commodities for the Space Launch System in response to automated and manual commands, safely as desired; preventively and responsively to adverse conditions, during initial integration and checkout, and during launch operations.**				
3	TS&R				
4	**Supporting Statements**	**S/W ?**	**Scope Rati**		**xt (optional)**
11	Perform Functional Verification	y	Command processing, display indicators	Sec 1.1	XXXXXXXXXXXXXXX
12	Perform Cryos Electrical Checkout	y	Software used to display readings/indicators	Sec 1.1	XXXXXXXXXXXXXXX
13	Perform HazGas Leak Detection	y	Uses HGDS system w/software	Sec 1.1	XXXXXXXXXXXXXXX
18	Perform Pneumatic Checks	y	Software used to control valves, monitor status	Sec 1.1	XXXXXXXXXXXXXXX

Requirements					Test												
3.1	3.2	3.3	3.4	3.5	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1
Y	X	X	X	P	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X

Coarse filter – if it's not Software, it's not in scope

GMPS Assurance Stmts

The New Approach – Continued

	A	B	E	F	G
1	**Top-level Claim**				
2	**The Ground Main Propulsion System software will monitor and control propellent and fluid commodities for the Space Launch System in response to automated and manual commands, safely as desired; preventively and responsively to adverse conditions, during initial integration and checkout, and during launch operations.**				
3	TS&R				
4	**Supporting Sta**			**ConOps Ref**	**Original Text (optional)**
11	Perform Functional Verification	y	Command processing, display indicators	Sec 1.1	XXXXXXXXXXXXXXX
12	Perform Cryos Electrical Checkout	y	Software used to display readings/indicators	Sec 1.1	XXXXXXXXXXXXXXX
13	Perform HazGas Leak Detection	y	Uses HGDS system w/software	Sec 1.1	XXXXXXXXXXXXXXX
18	Perform Pneumatic Checks	y	Software used to control valves, monitor status	Sec 1.1	XXXXXXXXXXXXXXX

Requirements					Test												
3.1	3.2	3.3	3.4	3.5	4.1.1	4.1.2	4.1.3	4.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1
Y	X	X	X	P	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X

Link to Source Doc

GMPS Assurance Stmts

New Approach (cont)

Forward link to Issues

Test									Design						Implementation					
.1.4	4.1.5	4.2	4.3	4.4	4.5	4.6	4.7	4.8	5.1	5.2	5.3	5.4	5.5	5.6	6.1	6.2	6.3	6.4	6.5	6.6
BD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	X	X	Y	P	X	TBD	TBD	TBD	TBD	TBD	TBD	TBD

ConOps Ref	Original Text (optional)	Project Concurrence	SRDS Ref	Comments/notes on SRDS References	Display Name	Open TIMs
Sec 1.1	XXXXXXXXXXXXXXX		7.1.11 7.1.12		MPS_Display_24	
Sec 1.1	XXXXXXXXXXXXXXX		Not found	Need to find where CLLS lives		
Sec 1.1	XXXXXXXXXXXXXXX		6.1.3		MPS_Display_18	
Sec 1.1	XXXXXXXXXXXXXXX		6.1.3		MPS_Display_18	

New Approach – Analyst's worksheet

	C	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	**Source Data**															**Analysis Data**	
2		**Reqt Category Checklist**				**Analysis Checklist**											
3	**Reqt Text**	Desired	Preventive	Responsive	Inferface	Correct	Unambiguous	Complete	Consistent	rifiable	n Independent	ble	Have SRDS/KGCS IF/GIS	istency	rement is accurately sented in the design rements SET Completeness	ance Statement Link	Candidate Issue (y/n)
4	GMPS_0001 - GMPS Shall display pressurization command buttons and feedback for GHE750 subsystem, as defined in table 7.1 Section 7.1.11	Y					Y		Y				?			Y	
5	GMPS_0002 - GMPS Shall navigation buttons as defined in table 7.2 Section 7.2															Y	
6	GMPS_0003 - GMPS Shall display Cryos Electrical panel status, as defined in table 6.3.1 Section 7.1.11															N	
7	GMPS_0003 - GMPS Shall perform pressurization commands and feedback for GHE750 subsystem Section 7.1.11															Y	

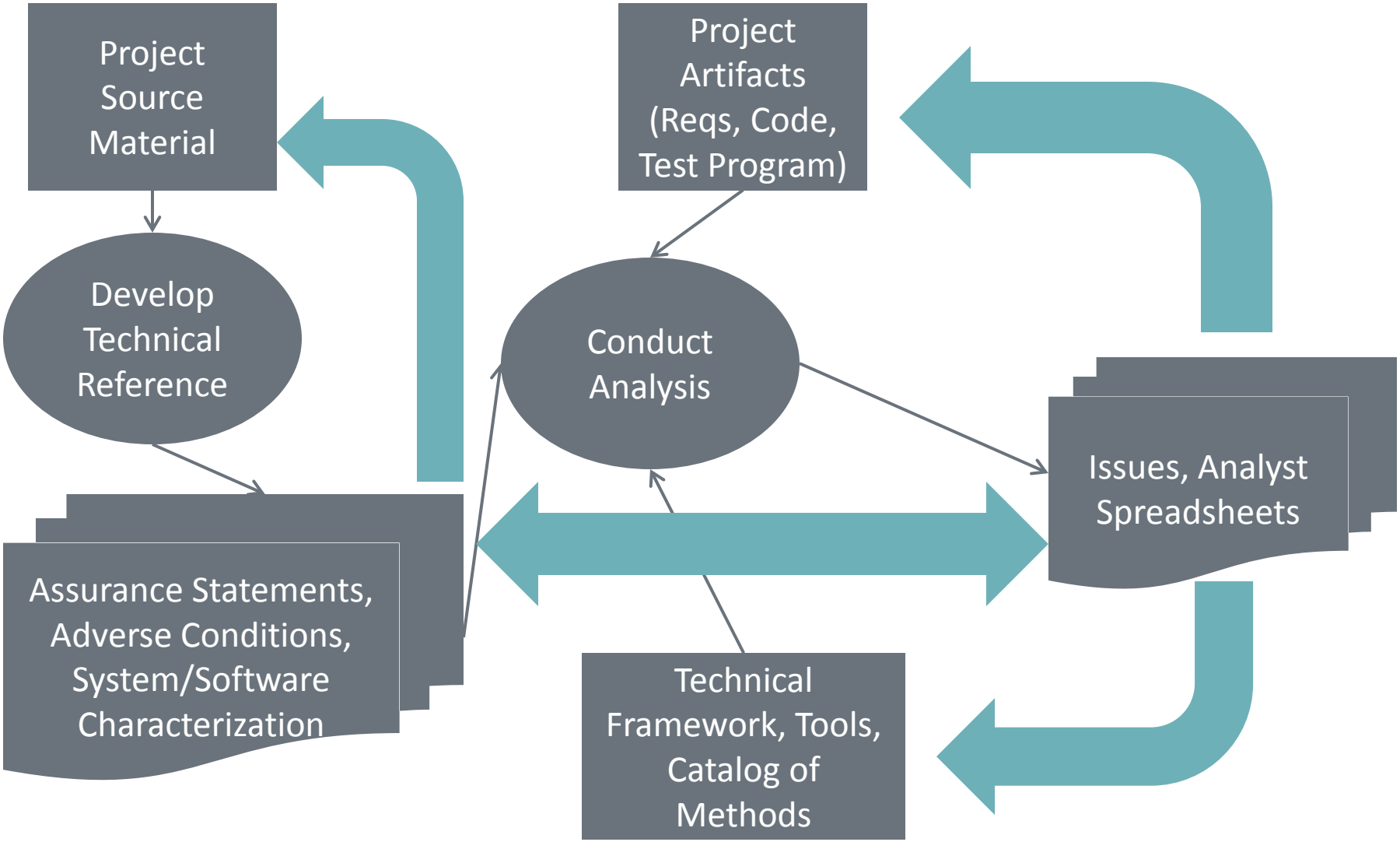
Section and Requirement Serve as major and minor keys

Backward link to Assurance Statements

New Approach – Analyst's worksheet (cont)

P	Q	R	S	T	U	V	W	X	Y	Z	AA
Analysis Data											
Analysis Checklist								Issue			
Consistent	Verifiable	Design Independent	Feasible	CUIs Have SRDS/KGCS IF/GIS Consistency	Requirement is accurately represented in the design	Requirements SET Completeness	Assurance Statement Link	Candidate Issue (y/n)	Issue #	Issue Description	Analysis and Validation Comments
Y	Y			?			Y		1381	Cut-and-pasted from issue repository	
							Y		1394	Cut-and-pasted from issue repository	
							N				Missing Artifact

Issues Support Assurance and Project's Perspective



Results

- Established bi-directional tracing of assurance evidence, via assurance statements, with minimal impact to current spreadsheets
- Rather time-intensive.
  - There is no half-way on this. You either enter the information and therefore have traceability, or you don't
- Still lots of features to add
  - Automatic roll-up of
    - Issues into assurance summaries
    - Goodness
    - Reporting of residual risk from missing artifacts
- Applicable to any Assurance Case component – e.g., Test Program!
  - Project requirements number remains as logical key
- Could be implemented in a data base.
- Evidence Based Assurance is directly supportable without reinventing the wheel.

Wrap-up

- Questions?
- Email – patrick.m.olguin@nasa.gov
- Phone – 562.682.5167
- Links to actual examples, users guide – available by request
- Acknowledgements
  - Sam Brown, Scott Schield – Keylogic
  - Karen Aument, Mike Perry – GSDO
  - Travis Dawson - TASC