JAXA's IV&V Activity and Value Concept

JAXA IV&V team
Hiroki Umeda, Tsutomu Matsumoto,
Naoko Okubo, Masa Katahira
okubo.naoko@jaxa.jp
2013/09/10

Contents

Brief history of IV&V activities in JAXA

Start of IV&V

(over decades ago)

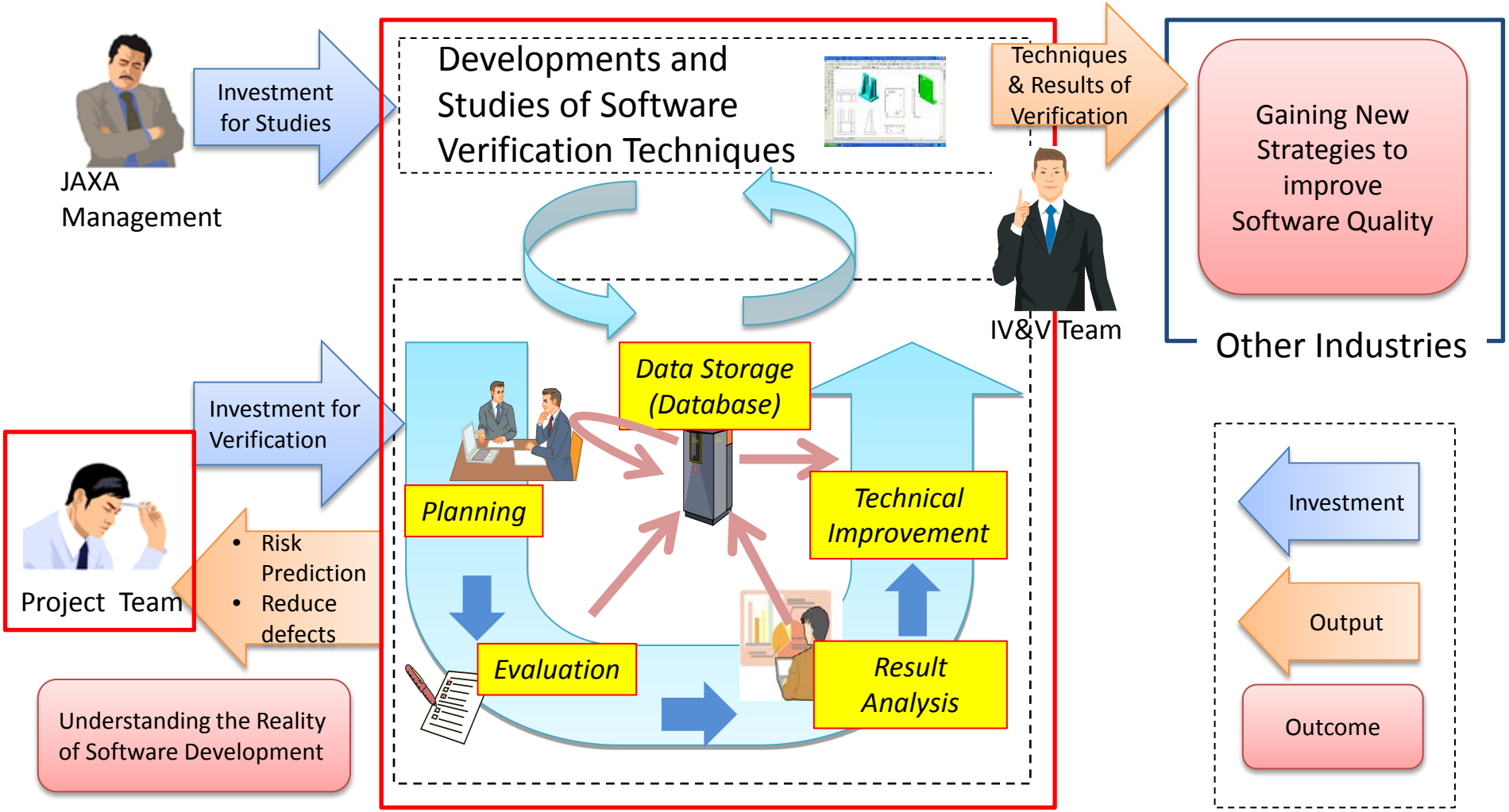
Apply to various projects

NOW

IV&V Program become widespread
→ NEEDS are changed

Characteristics of JAXA's IV&V Program

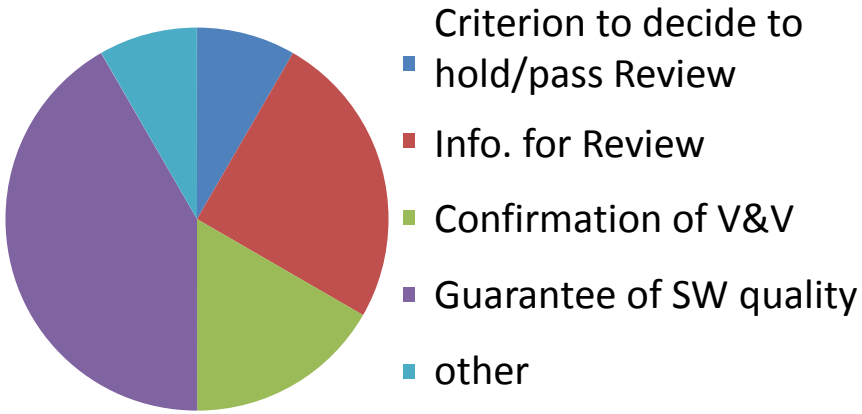
- Beneficiaries pay IV&V costs (Projects have funds).
- IV&V is finished when a result is reported to a project team.



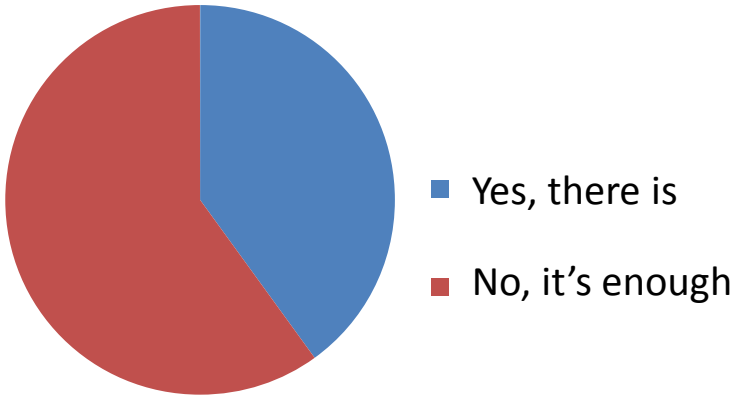
Examples of Project's Request

- The Result of the Questionnaire to five projects, which used IV&V program in 2012

Q1: How do you use IV&V in your SW development pass?



Q2: Is there a room for improvement for IV&V Finding lists?



KEYWORDS

1. Confidence
   - ✓ Can move on to next milestone or not?
2. Guarantee
   - ✓ Outcome SW
3. Improvement
   - ✓ Show the results effectively (ex. Show the risk for operation)

Clarification of IV&V NEEDS

- NEEDS 1: Clear accountability for "Confidence"
- NEEDS 2: "Guarantee" the SW quality as a whole
- NEEDS 3: Show traceability between SW defects on orbit and operational risks.

BEFORE

- Figure out significant problems of software development.
- Understand verification attributes and scope of IV&V.
- Finish up with merely identifying the problems.

NOW

Confidence

- Gain a future advice and judgment stuff for development which can be learned from software defects.

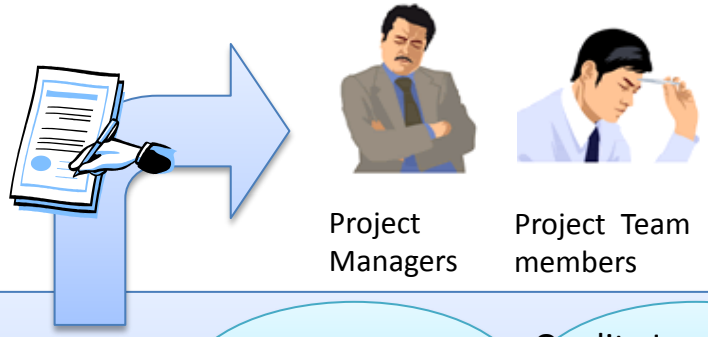
Guarantee

- Know how much IV&V contributed to the high-reliable software together with V&V.

Improvement

- Understand how software problems influence on operations. Traceability between software defects and risk for operations is required.

Overview of New IV&V Value Concept



- ✓ Clear Accountability for confidence
- ✓ SW Quality Improvement
- ✓ Understand defects and its effect easily

Visualization

Outcomes of IV&V activities

- Quality Visualization
- Quality Improvement of Development Products
- Identification of Technical Failure

Project Milestone: Requirements Phase → Design Phase → Coding Phase → Test Phase

Expectations for IV&V Activities: Predicting Risks → Removing Problems

Optimization

IV&V Team

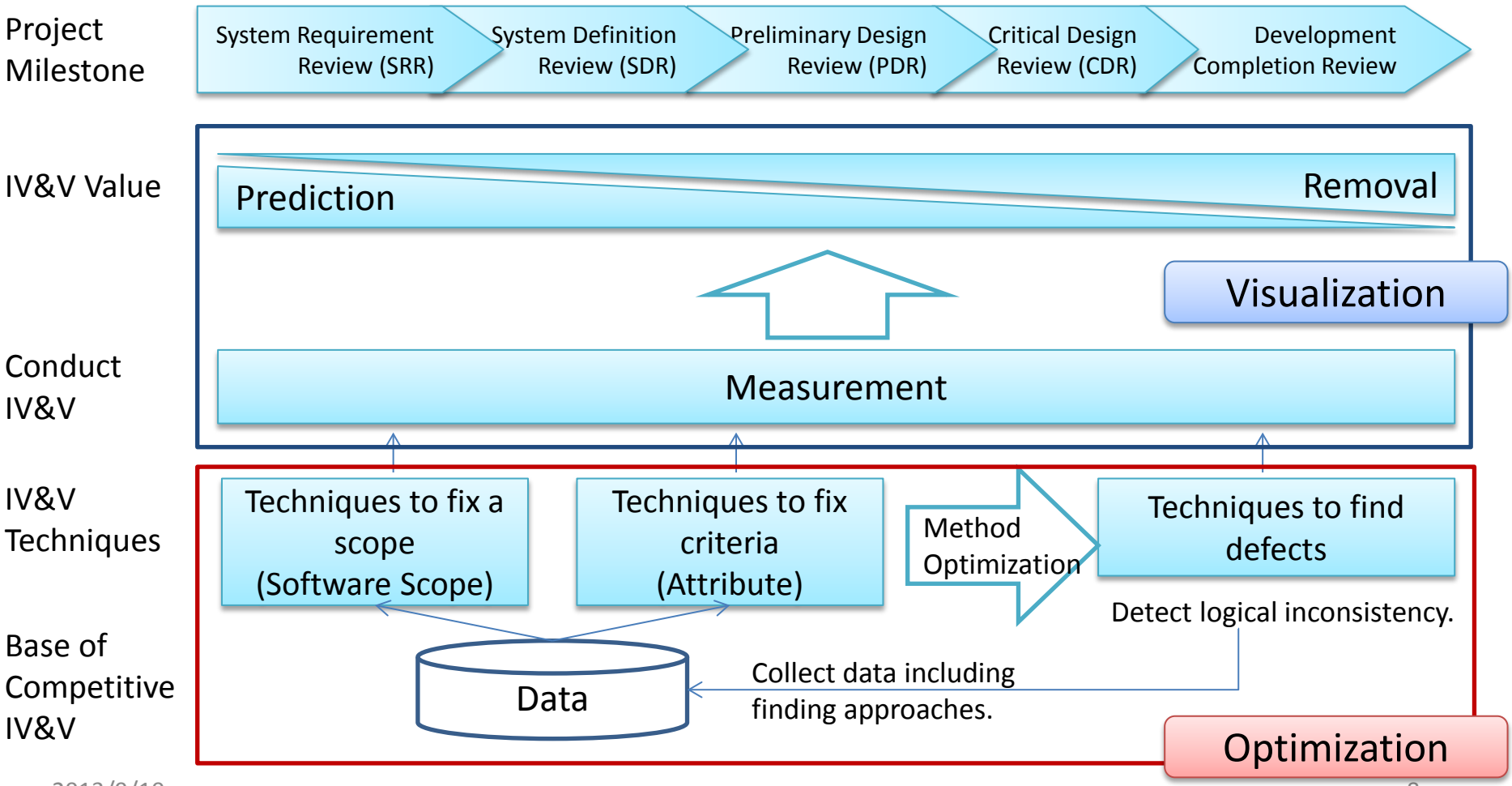
Storage of Cost-benefit Data per Attribute/Method

Analysis of Characteristics of the Target Products

Use IV&V knowledge across projects.	• Store information of identified problems.
Set verification attributes from a system-building/operational viewpoint.	• Define verification attributes after identifying important functions and scenes in missions or operations.
Establish verification techniques different from developers.	• Improve IV&V Manual, make use of Formal Method, etc.

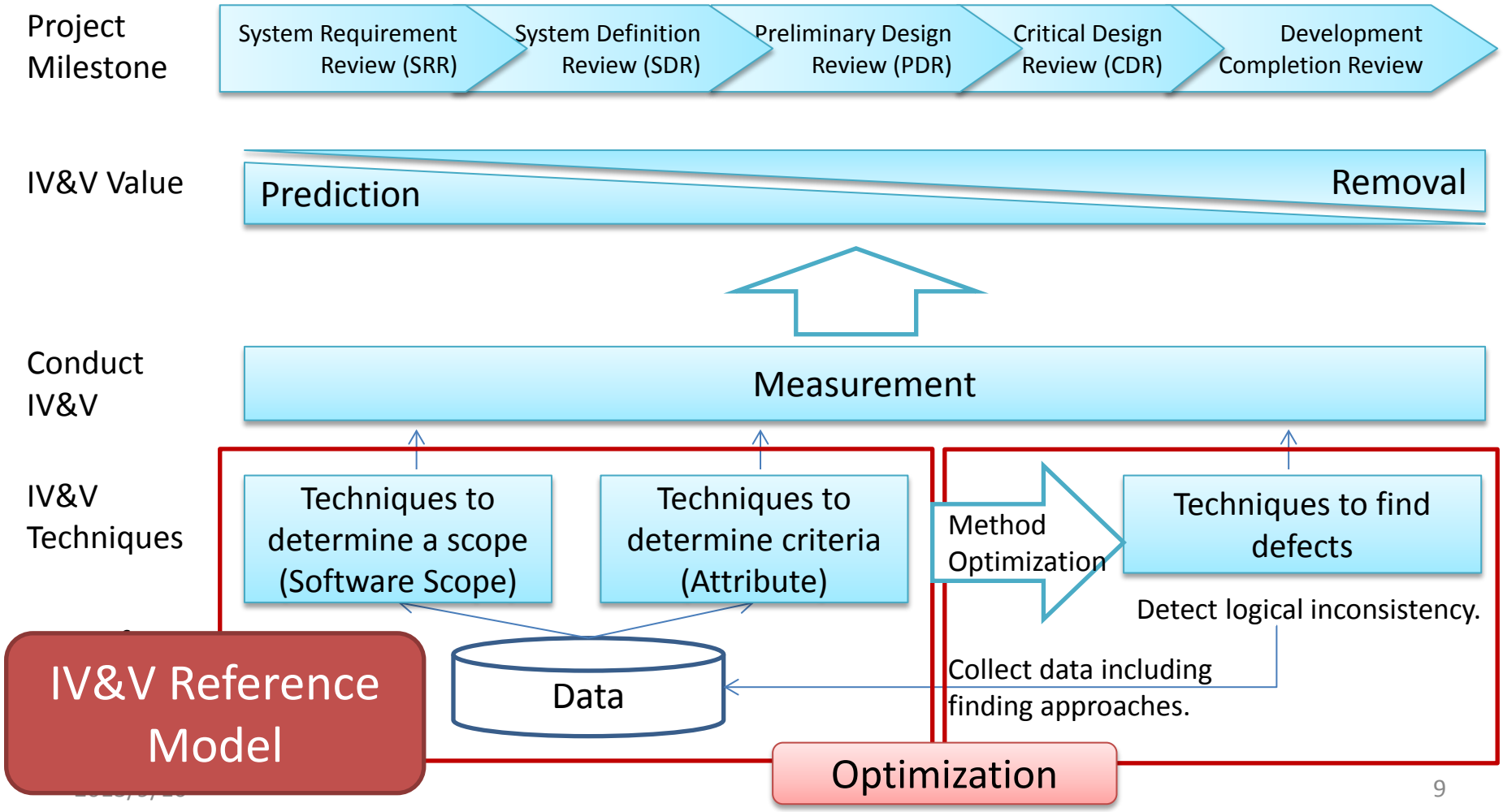
Issues of New IV&V Value Concept

- Visualization : How to present the result effectively to Project?
- Optimization : How to find defects efficiently?



Detail of Optimization

- Effective way to collect and use Data (Left part of Fig.)
- Suitable method to find defects (Right part of Fig.)



Attempt of IV&V Reference model

- IV&V Reference Model:
  Normalized Model/Method to clarify defects and risks
  1: Stable IV&V Quality
  2: Comparable with other SW, or projects
  3: Improvement of persuasion

- Issues for defects/risks clarification

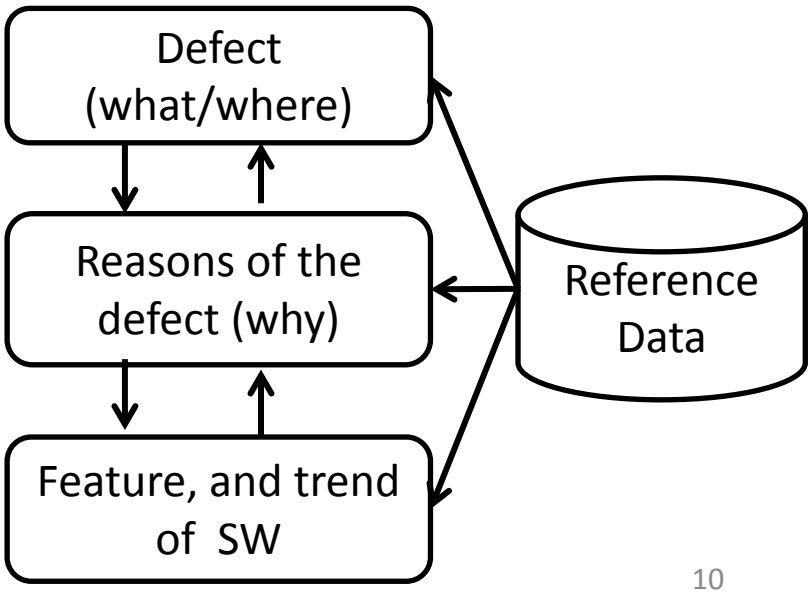
Before

How to describe defects/risks depends on individual IV&V engineers.

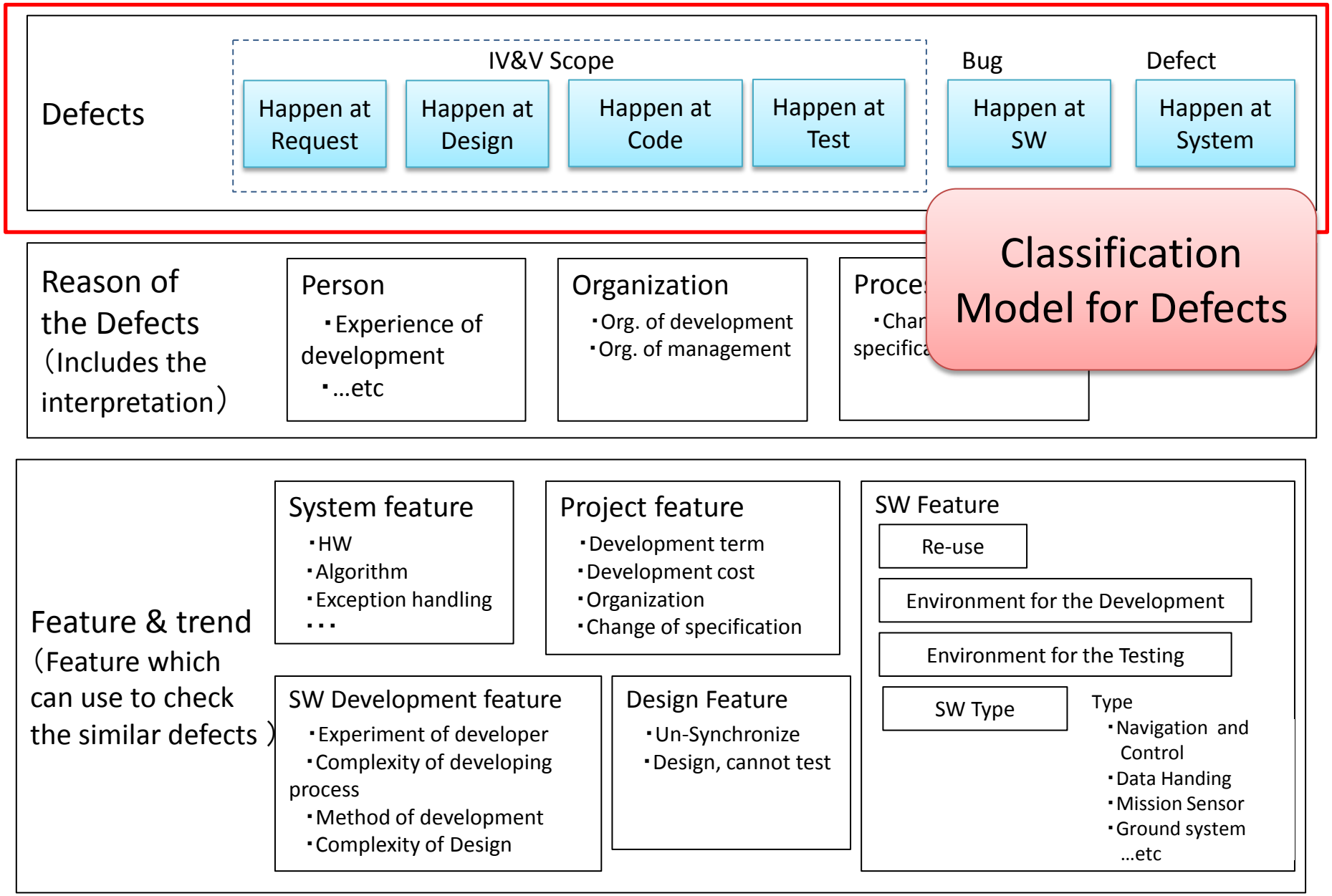
Hard to …
- ✓ understand promptly
- ✓ compare with others
- ✓ convince the projects

IV&V Reference Model

- Describes the defect and risk using reference data



Factors of IV&V Reference Model



Attempt of Defect Classification Model

No.	Types of Defects	Details	Error	lack	Unclear -ness	Inconsist -ency	Examples
1	Functionality Definition	Errors related to definition of system processing. Lack of definition of the subject function etc.	○	○	—	—	・Lack of functionality
2	Data Definition	Errors related to data definition. Inconsistent common commands, lack of definition of the subject data, unclear specification about debug commands, etc.	○	○	○	○	・Lack of data definition
3	Processing Logic	Errors related to processing logic/order. Wrong order of processing main/sub tasks, wrong setting with no loop, etc.	○	—	—	—	
4	Mode Transition	Errors related to system mode transition. Wrong space where the mode transit to, missing definition of transition conditions, etc.	○	○	—	—	
5	Exception Handling	Errors related to exception or error handling in system malfunction. Unclear behaviors when receiving unintended data, missing definition of error handling, etc.	○	○	○	—	
6	Timing (Synchronization/ Exclusive Processing)	Errors related to timing between functions or between hardware and software. Inconsistency of sending and receiving timing etc.	○	—	—	○	

Attempt of Defect Classification Model

No.	Types of Defects	Details	Error	lack	Unclear -ness	Inconsist -ency	Examples
7	Boundary Value	Errors related to boundary values in data. Validity of a scope of memory clearance, etc.	○	–	–	–	
8	Constant Value/ Initial Value	Errors related of constant values and initial values of variables. Mismatch of constant values between specifications, missing initial values of a program, etc.	○	–	–	○	・Error in input value of data
9	Ambiguous Description	Errors of description in a subject specification which are not related to a system itself. Clerical errors, wrong page/revision numbers, etc.	○	–	–	–	
10	Integrity with Hardware	Errors related not just to software but to integrity with onboard hardware. Mismatch of specifications between software and hardware, lack of control when powers become excessive, etc.	○	○	–	○	
11	Inconsistency between Specifications	Errors related to consistency between a subject document and an upper specification or reference. Items defined in the upper specification are not correctly represented in the subject document, definition is missed in the upper one, etc.	○	○	–	○	

Conclusion

- Change of IV&V NEEDS
- Proposed New IV&V Value Concept
- Issues for New IV&V Value Concept
  - Visualization
  - Optimization (Attempt of IV&V Reference Model)

- Future work

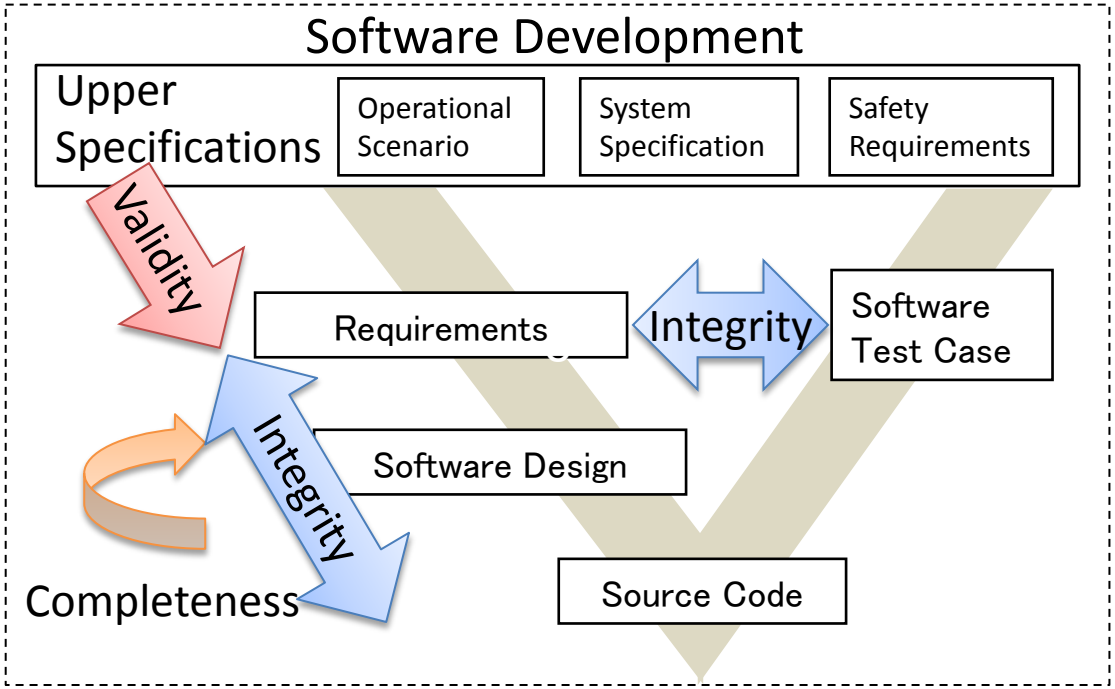
- Goal of IV&V is to improve operability (usability) by checking consistency between SW design and operation.
  → Analysis with an operational view and define outputs for them

- Make IV&V training course. Also, define required skills needed as IV&V engineer.

No.	Types of Defects	Details	Error	lack	Unclear -ness	Inconsist -ency	Examples
1	Functionality Definition	Errors related to definition of system processing. Lack of definition of the subject function etc.	○	○	—	—	・Lack of functionality
2	Data Definition	Errors related to data definition. Inconsistent common commands, lack of definition of the subject data, unclear specification about debug commands, etc.	○	○	○	○	・Lack of data definition
3	Processing Logic	Errors related to processing logic/order. Wrong order of processing main/sub tasks, wrong setting with no loop, etc.	○	—	—	—	
4	Mode Transition	Errors related to system mode transition. Wrong space where the mode transit to, missing definition of transition conditions, etc.	○	○	—	—	
5	Exception Handling	Errors related to exception or error handling in system malfunction. Unclear behaviors when receiving unintended data, missing definition of error handling, etc.	○	○	○	—	
6	Timing (Synchronization/ Exclusive Processing)	Errors related to timing between functions or between hardware and software. Inconsistency of sending and receiving timing etc.	○	—	—	○	

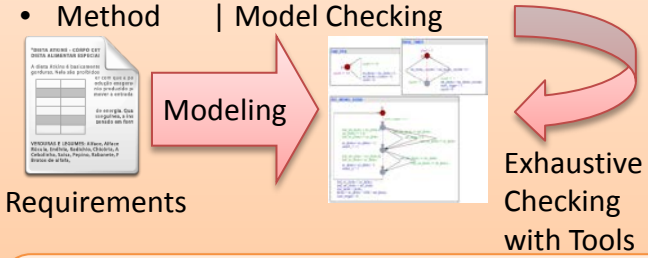
No.	Types of Defects	Details	Error	lack	Unclear -ness	Inconsist -ency	Examples
7	Boundary Value	Errors related to boundary values in data. Validity of a scope of memory clearance, etc.	○	—	—	—	
8	Constant Value/ Initial Value	Errors related of constant values and initial values of variables. Mismatch of constant values between specifications, missing initial values of a program, etc.	○	—	—	○	・Error in input value of data
9	Ambiguous Description	Errors of description in a subject specification which are not related to a system itself. Clerical errors, wrong page/revision numbers, etc.	○	—	—	—	
10	Integrity with Hardware	Errors related not just to software but to integrity with onboard hardware. Mismatch of specifications between software and hardware, lack of control when powers become excessive, etc.	○	○	—	○	
11	Inconsistency between Specifications	Errors related to consistency between a subject document and an upper specification or reference. Items defined in the upper specification are not correctly represented in the subject document, definition is missed in the upper one, etc.	○	○	—	○	

Software Development



■Case 1

- Target | Mode Transition in Software Requirements
- Attribute | Verification of Completeness
- Method | Model Checking



■An Example of Identified Problems
Mode Transition could stop because some conditions executing safety mode transfer function were not sufficient.

IV&V Activities

Define a target or attribute of verification

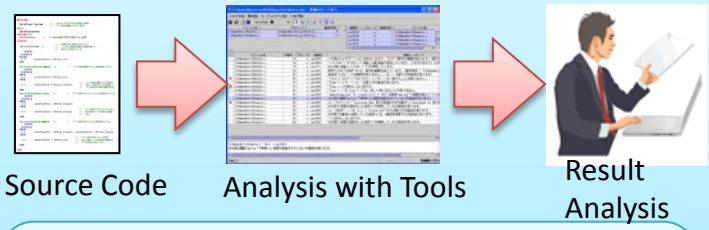
Select technique to detect problems

Set an attribute of verification (Integrity, Completeness, etc.) for each development phase based on IV&V Manual.

Techniques	Requirement Analysis	Design	Coding	Test
System/Safety Analysis	○			
Check List	○	○	○	○
Model Analysis	○	○		
Model Checking	○	○	○	
Static Code Analysis, Structure Analysis			○	
Independent Testing			○	○

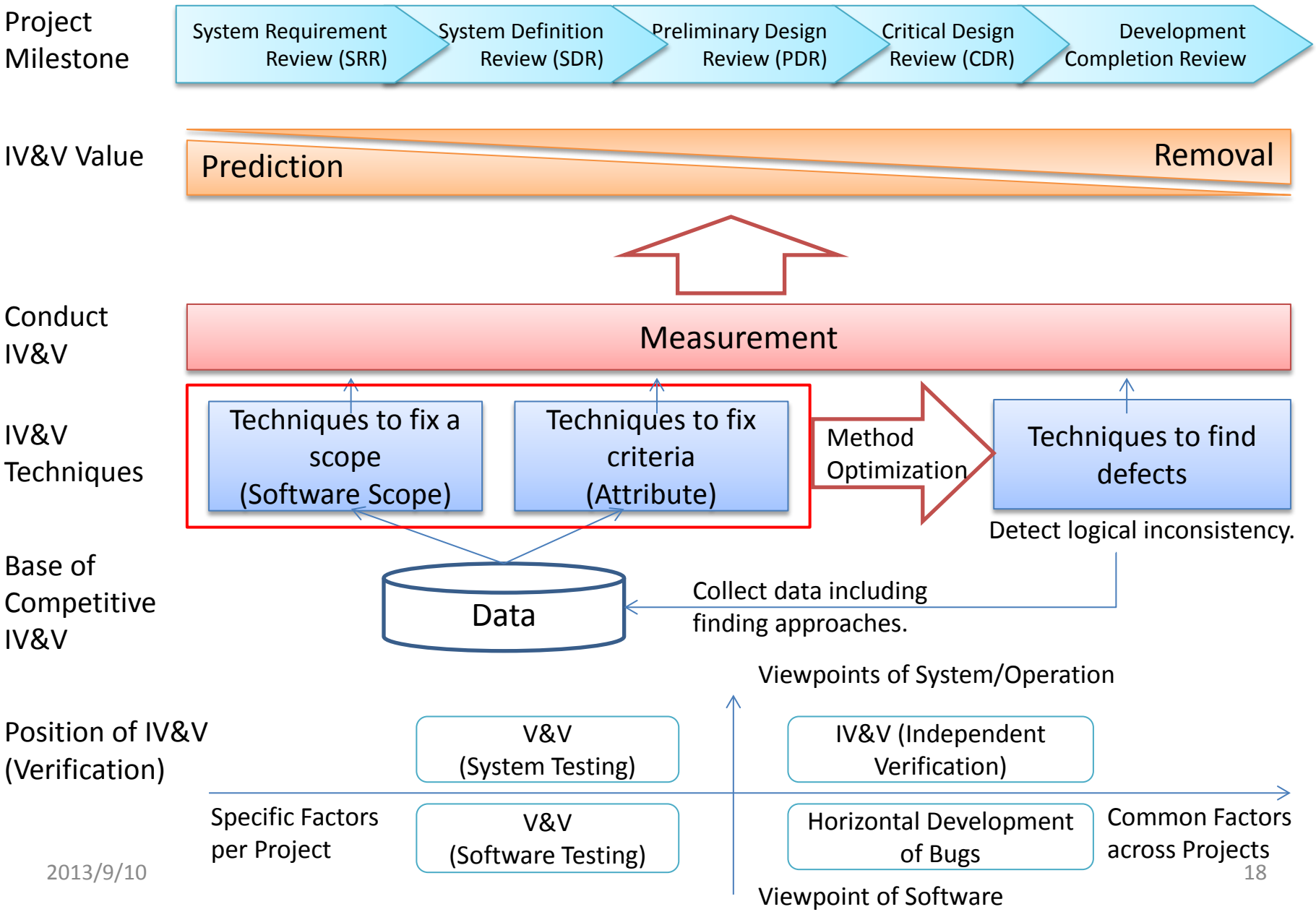
■ Case 1

- Target | Asynchronous Processing (Interrupt) in Source Code
- Attribute | Verification of Integrity
- Method | Static Analysis



■An Example of Identified Problems
Some processing could conflict with others when doing interrupt mask in Source Code, because some function calls were missing.

IV&V Value (1)


Project Milestone
System Requirement Review (SRR)
System Definition Review (SDR)
Preliminary Design Review (PDR)
Critical Design Review (CDR)
Development Completion Review
IV&V Value
Prediction
Removal
Conduct IV&V
Measurement
IV&V Techniques
Techniques to fix a scope (Software Scope)
Techniques to fix criteria (Attribute)
Method Optimization
Techniques to find defects
Detect logical inconsistency.
Base of Competitive IV&V
Data
Collect data including finding approaches.
Position of IV&V (Verification)
Viewpoints of System/Operation
V&V (System Testing)
IV&V (Independent Verification)
Specific Factors per Project
V&V (Software Testing)
Horizontal Development of Bugs
Common Factors across Projects
Viewpoint of Software

3 Issues to Achieve New IV&V Value Concept

Keywords	Policy	Supplement
Visualization	• Explanation of cost-effectiveness • Risk-based analysis	• Prepare convincing explanations and indicators for projects (developers) and end customers. → A new usage of outcomes of IV&V. Improve stakeholder satisfaction. • Appeal and transfer of techniques to other industries. Provide the activity, techniques, data and training materials.
Differentiation	• Reinforcement of unique viewpoints • Utilization of actual data	• Focus not on the number of methods but on their quality. • Apply methods to collect data. • Collected data of defects, bugs and findings of each software with background information such as factors are available for IV&V.
Automation	• Standardization of methods and processes • Utilization of tools	• Processes and outputs are standardized. → Verification can be done by more than one engineer.