COCOMO® III Update

Brad Clark, PhD

USC Center for Systems and Software Engineering

2018 Annual Research Review

March 14, 2018

Topics

- Required Security for Software Development
- New Nominal
- Model Definition Manual - Beta
- Next steps

Required SW Security (SECU)

- **New security cost driver added to COCOMO III**
  - **Address the cost of developing software to be *resilient* to unauthorized disclosure or attack**
- **Two draft standards were used to provide security information used in the assessment**
  - **Lifecycle Requirements: ISA-62443-4-1 Secure Product Development Lifecycle Requirements**
  - **Component Requirements: ISA-62443-4-2 Technical Security Requirements for Industrial Automation And Control Systems (IACS) Components**
- **Two workshops were held to assess how development lifecycle and software component requirements would be handled by COCOMO III**
  - **Participants (12) were asked to identify where the model addressed security lifecycle and component requirements.**
  - **3 Votes for a model parameter required to be considered for model modification**

ISA: International Society of Automation

SECU Rating

- **These rating scales describe the level of security based on unauthorized disclosure or attack. The higher the rating, the more rigorous the practices and the more complex the implementation for the security requirements (next two slides).**

Rating	Very Low	Low	Nominal	High	Very High	Extra High
SECU	N/A	None	Prevent unauthorized disclosure using casual eavesdropping or casual exposure	Prevent unauthorized disclosure using simple means with generic skills	Prevent unauthorized disclosure using sophisticated means but moderated resources	Prevent unauthorized disclosure using sophisticated means and extended resources

- **Other cost drivers in this model account for additional effort required for security practices.**

SW Lifecycle Requirements

- **Security management:** ensure that the security-related activities are adequately planned, documented and executed throughout the product's life-cycle
- **Specification of security requirements:** document the security capabilities that are required for a product along with the expected product security context (authentication, authorization, encryption, etc.)
- **Secure by design:** ensure that the product is secure by design including defense in depth. *Defense in depth* provides one or more layers of security to thwart security threats
- **Secure implementation:** ensure that the product features are implemented securely
- **Security verification and validation testing:** security testing required to ensure that all of the security requirements have been met
- **Security defect management:** ensure the handling security-related issues of a product that has been configured to employ its defense in depth strategy
- **Security update management:** ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner

Source: ISA-62443-4-1 Secure Product Development Lifecycle Requirements

SW Component Requirements

- **Identification and authentication control:** identify and authenticate all users and other software applications
- **Use control**: enforce assigned privileges of user or another software application
- **System integrity:** ensure integrity of the application to prevent unauthorized manipulation
- **Data confidentially**: ensure confidentiality of information and communication channels and prevent unauthorized disclosure
- **Restricted data flow:** segment the control system via zones and conduits to limit the unnecessary flow of data
- **Timely response to events:** respond to security violations by notification and reporting in a timely manner
- **Resource availability**: ensure availability of the application against degradation or denial of essential services

Source: ISA-62443-4-2 Technical Security Requirements for IACS Components

Secure Dev Impact on Drivers -1

- **Workload Size**
  - Identification / authentication control
  - Use control
  - Data confidentially
  - Restricted data flow
  - Timely response to events
- **Complexity**
  - Identification / authentication control
  - Use control
  - Data confidentially
  - Resource availability

Secure Dev Impact on Drivers -2

- **Process Capability**
  - Security management
  - Specification of security requirements
  - Secure by design
  - Secure implementation
  - Security defect management
  - Security update management
- **Applications Experience**
  - Security management
- **Use of Software Tools**
  - Security management
- **Development Flexibility**
  - Specification of security requirements
  - Security management
- **Platform Experience**
  - Timely response to events
- **Peer Reviews**
  - Specification of security requirements
  - Secure by design
  - Secure implementation
- **Software Architecture Understanding**
  - System integrity
  - Secure by design
  - Resource availability
- **Applications Experience**
  - **Secure by design**
  - Secure implementation
- **Execution Testing and Tools**
  - Security verification and validation testing

Topics

- Required Security for Software Development
- **New Nominal**
- **Model Definition Manual - Beta**
- **Next steps**

The New "Nominal"

- Cost Driver definition refinement

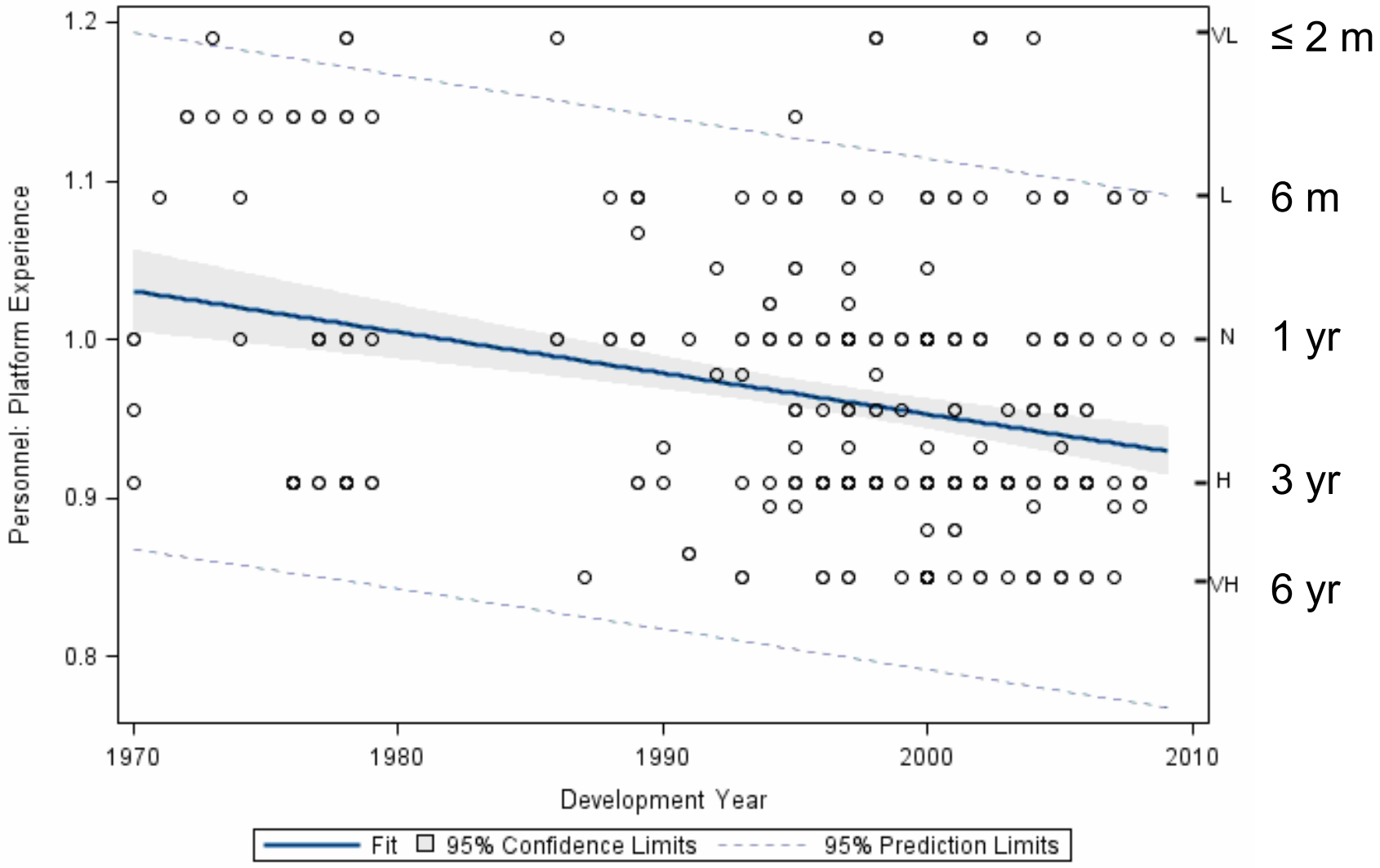
- The New "Nominal
  - Study of productivity trends over the past 40 years reveals a shift in "nominal" ratings
  - Following slides show the shift in ratings for selected cost drivers, i.e., the new "nominal"

Impact of Productivity Trends

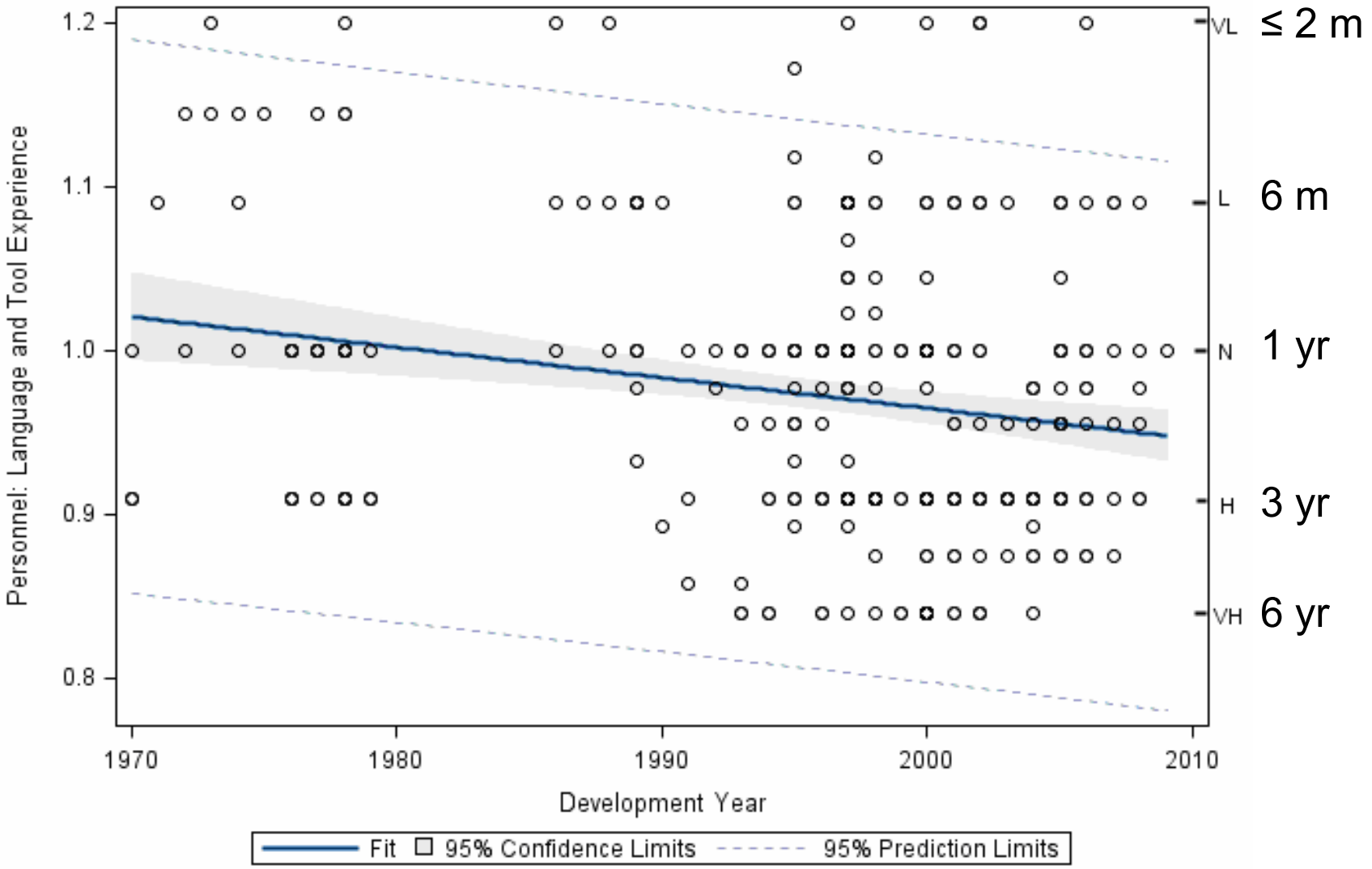
Kendall's Rank Correlation Coefficients between the Completion Year and COCOMO II Cost Drivers (sorted by degrees of correlation)

Cost driver Kendall's	τ	p-value
TOOL Use of Software Tools	-0.37	2.20E-16
PMAT Process Maturity (PCUS)	-0.30	1.22E-13
STOR Main Storage Constraint	-0.29	1.31E-11
TIME Execution Time Constraint	-0.26	6.62E-10
PLEX Platform Experience	-0.17	1.98E-05
PVOL Platform Volatility	-0.18	2.04E-05
APEX Applications Experience	+0.17	4.88E-05
LTEX Language and Tool Experience	-0.15	2.84E-04
~~DATA Database Size~~	+0.13	1.81E-03
RELY Required Software Reliability	-0.10	1.42E-02
CPLX Product Complexity	-0.10	1.58E-02
PREC Precedentedness of Application	-0.09	2.13E-02
ACAP Analyst Capability	+0.08	4.87E-02

Platform Experience-PLEX



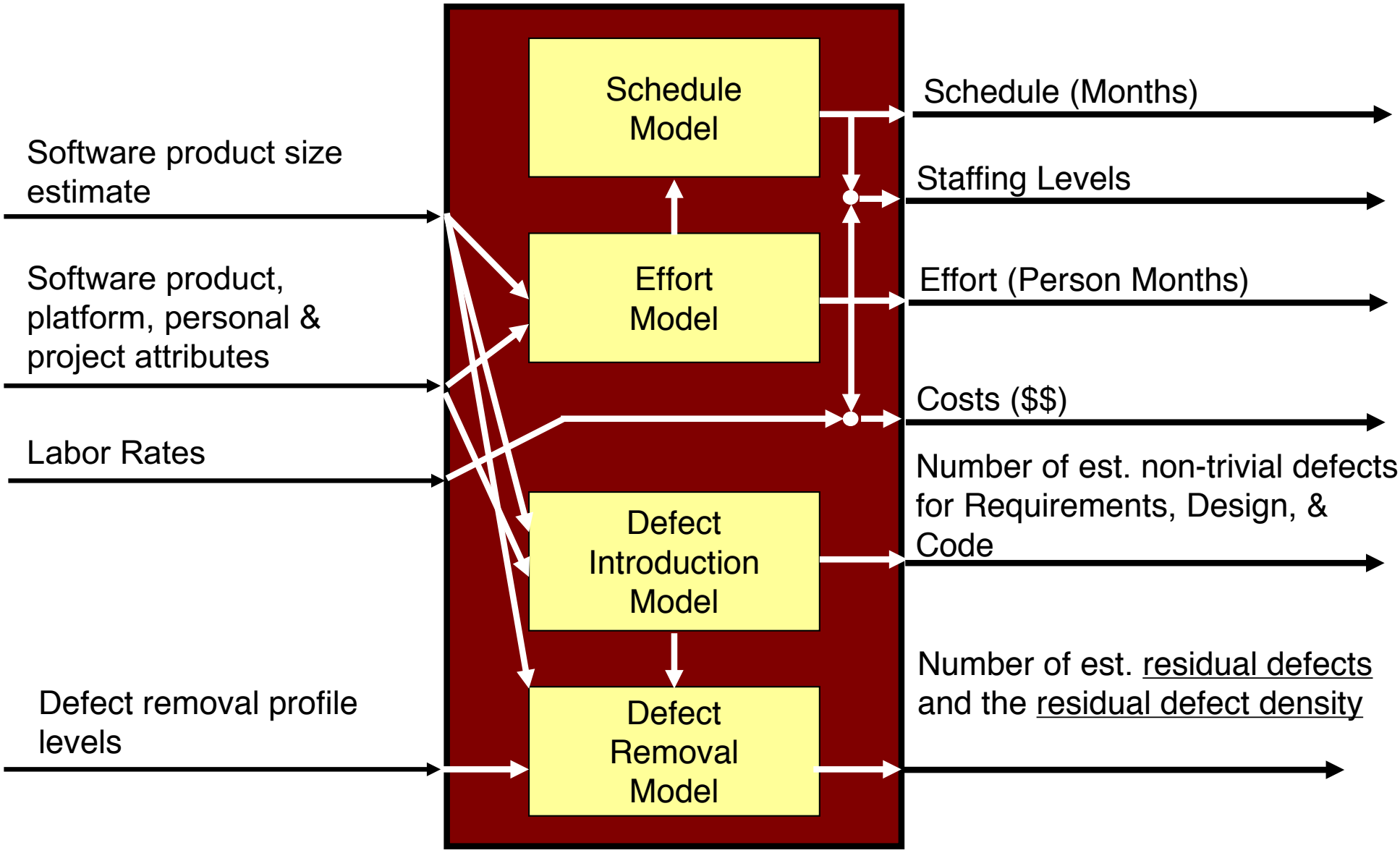
Language and Tool Experience-LTEX



Topics

- Required Security for Software Development
- New Nominal
- **Model Definition Manual - Beta**
- **Next steps**

COCOMO III Model Concept



Model Manual Overview

- Purpose
- Model Boundaries
- Model Workload Inputs
  - Function Points
  - COSMIC Function Points
  - Thousands of Source Lines of Code
    - New and Adapted Code
- Model Description
  - Model Specification
  - Application Super Domains (model pre-sets)
  - Six Baseline Cost Drivers (formally Scale Factors)
  - Fourteen Component Cost Drivers (formally Cost Drivers)
  - Three Quality Drivers (from the COQUALMO Model)
- Model Calibration
- Case Studies (e.g. multi-component estimation)
- Appendices (detailed description of cost drivers)

Next Steps

- **Next steps**
  - **Working group review of the model**
  - **Rosetta stone COCOMO II ➔ COCOMO III**
  - **Model performance analysis**
  - **Data collection**
    - **Form**
    - **Plan**