Cleanroom Software Engineering

MADE BY: HARSHITA SHARMA

UNIT 2

- Approach
- Functional Specification
- Design and Testing

THE APPROACH

What is it?

- Cleanroom
- Clean as you proceed
- Formal modelling and verification method
- Specialized specification approach
- Unique verification method
- rigourous

Why Cleanroom Software Engineering?

- What's the idea behind it?
- Advantages
  - Saved from rework
  - Less effort
  - Reduced cost
  - More robust software
- Emphasis on mathematical verification of correctness before coding
- Certification of software reliability
- Bottom line

Traditional strategy vs CSE

- Commencement
- Idea
- Cost
- Certifies reliability
- Flow

Representation

- Box structures
- Purpose: Encapsulation
- Step 1: Box structure designing
- Step 2: Correctness verification
- Step 3: Statistical usage testing

The Cleanroom Process Model

The Cleanroom Process Model

- Code Generation, Inspection and Verification
- Statistical Test Planning
- Statistical Use Testing
- Ceritfication

Modelling Activities

- Increment Planning
- Requirements Gathering
- Box Structure Specification
- Formal Design

Formal Verification Activities

- Correctness Verification
- Code Generation, Inspection and Verification
- Statistical Test Planning
- Statistical Use Testing
- Ceritfication

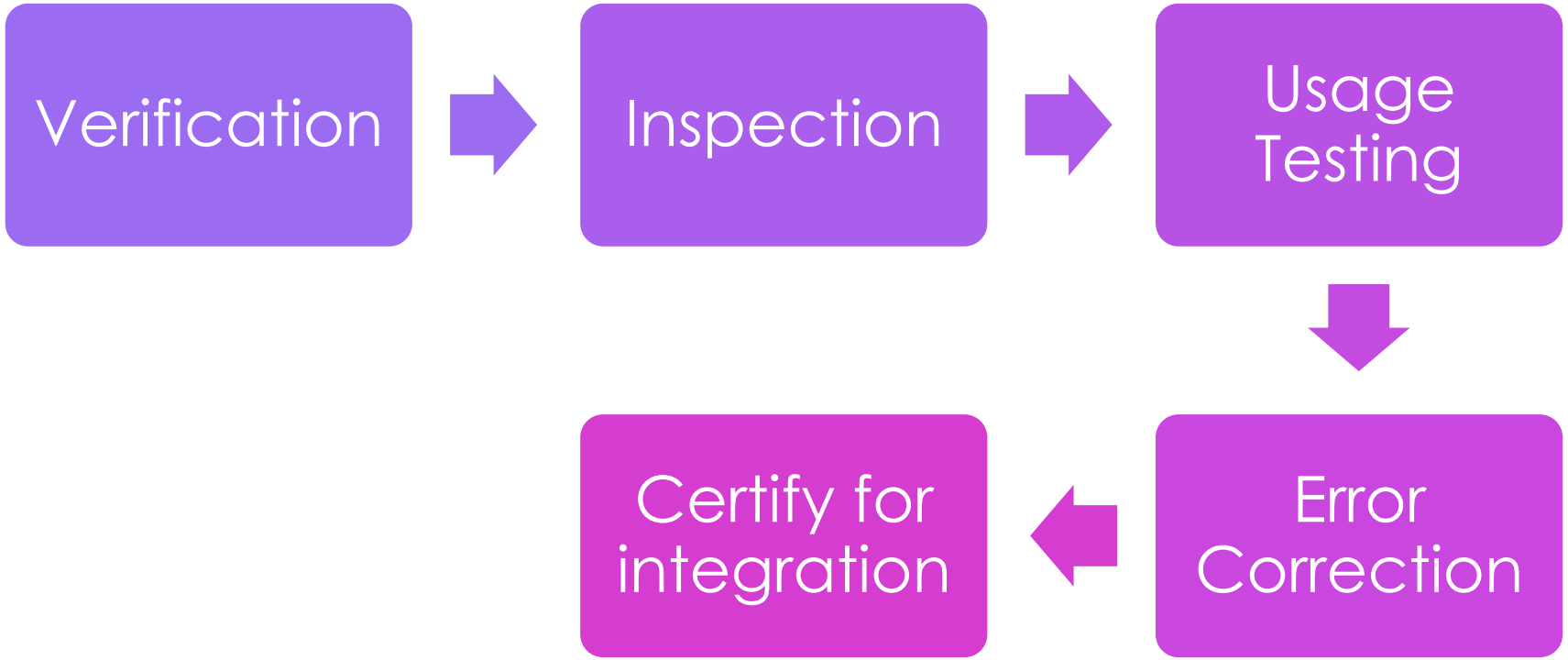
Code Generation, Inspection and Verification

Step 1 – BSS translated to Programming Language

Step 2 Technical Reviews (semantics and syntactic)

Step 3 Correctness verification of the source code

Certification

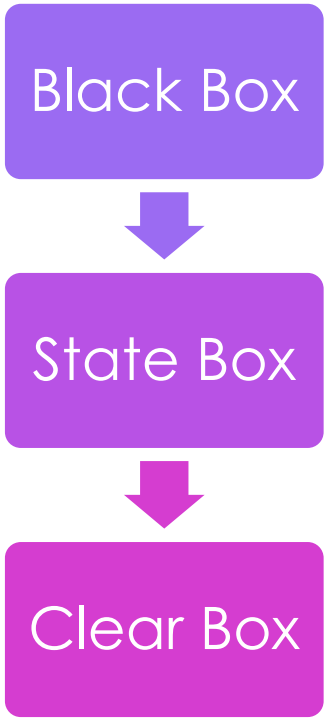


FUNCTIONAL SPECIFICATION

How is it done?

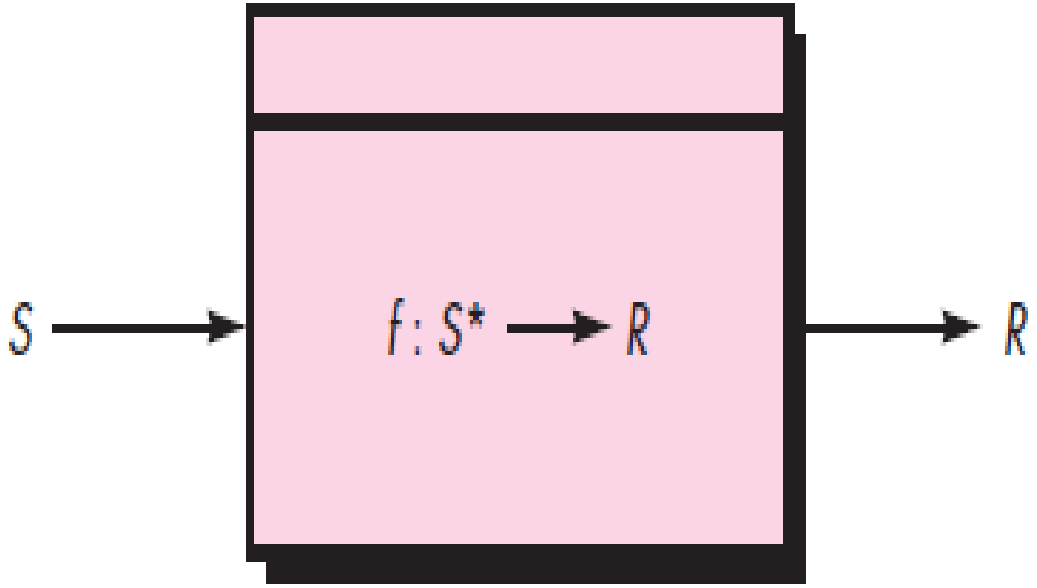
- Done by BSS
- Modelling activity
- What is a box?

Hierarchy of Box Refinement

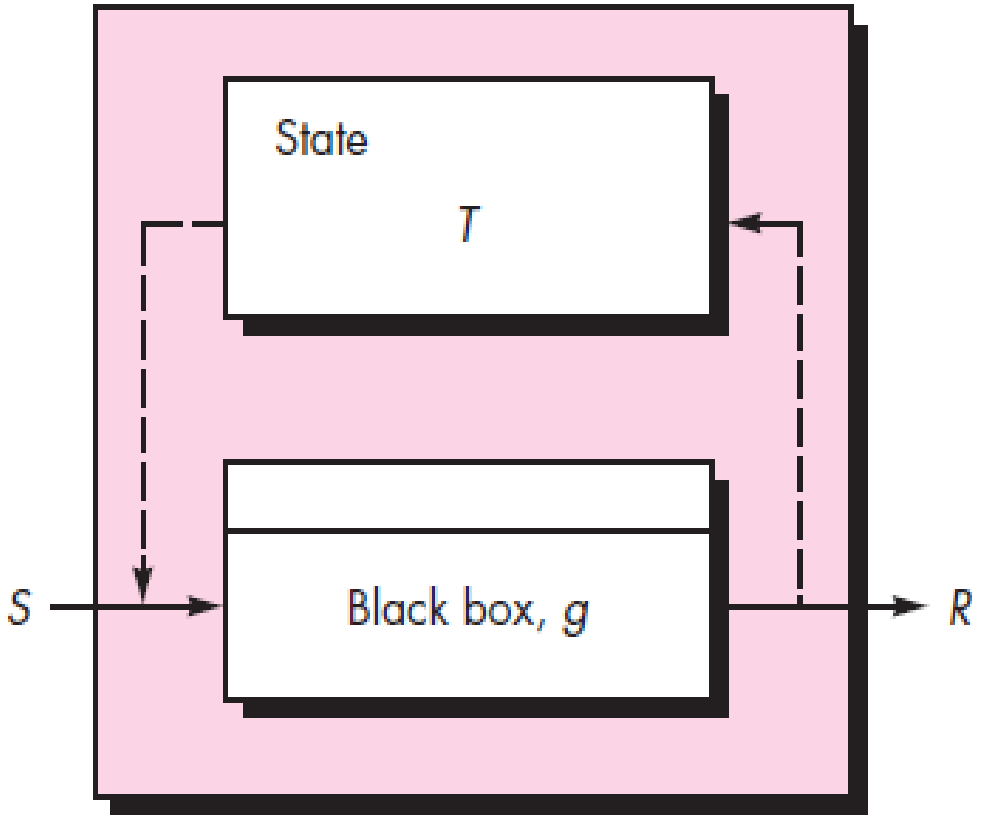


- Advantage – partition for analyst
- Property of each box – referential transparency

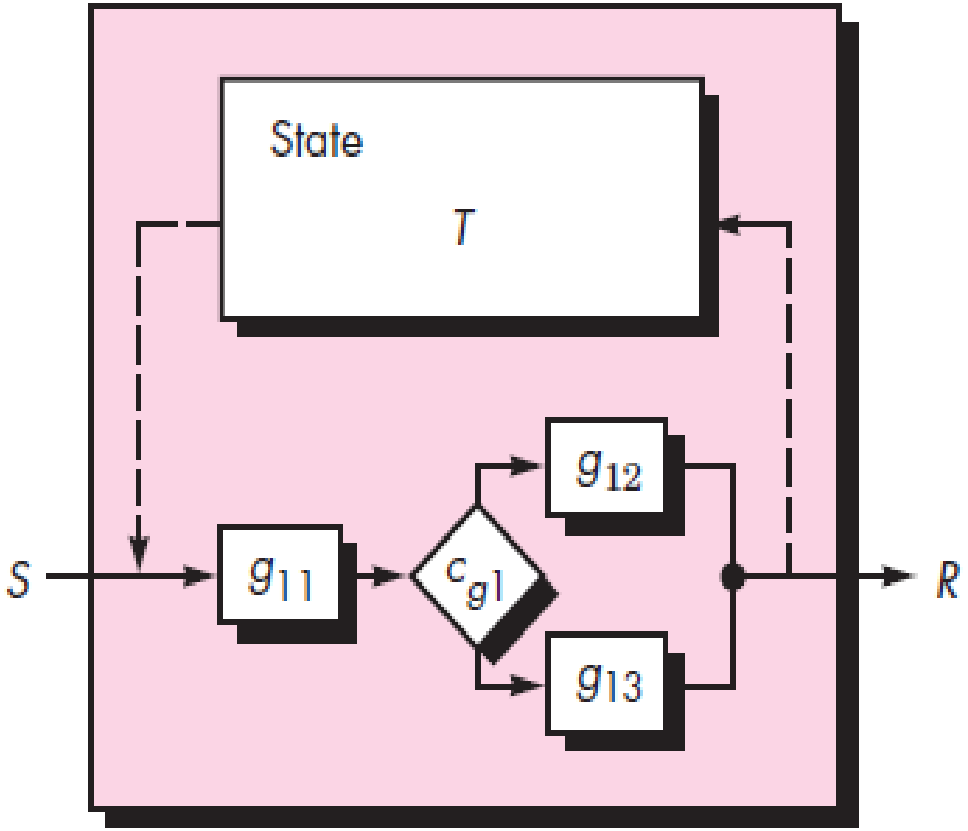
Black Box and its Specification



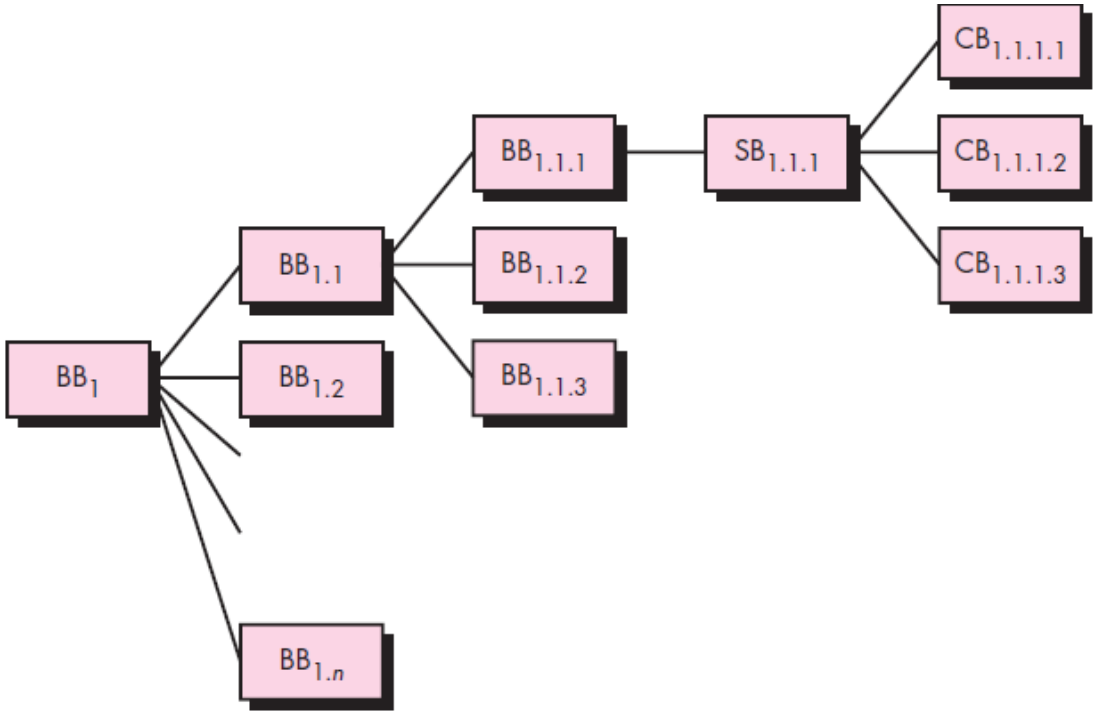
State Box and its Specification



Clear Box and its Specification



Refinement Approach using BSS



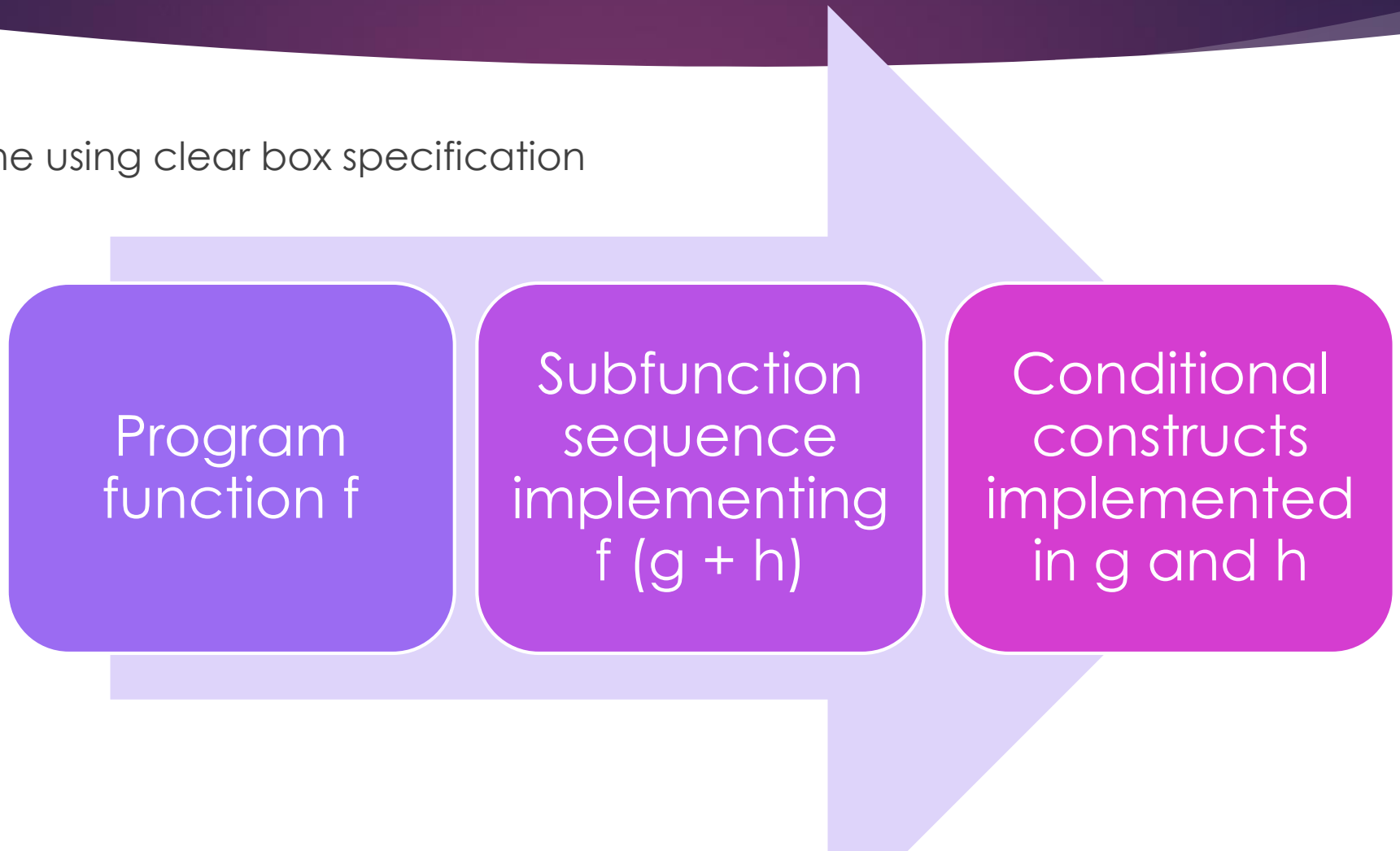
CLEANROOM DESIGN

Basics

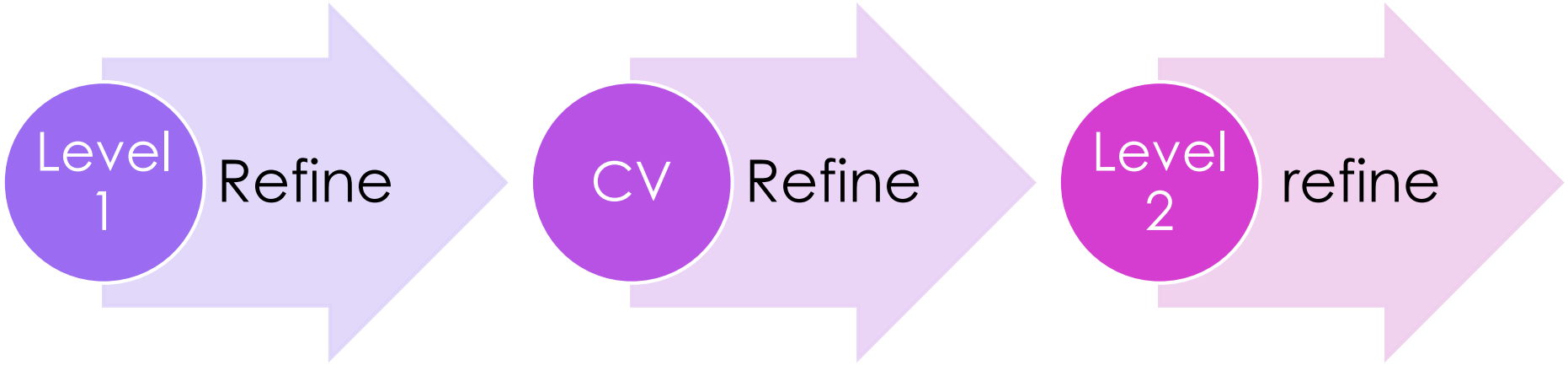
- Structured programming
- 2 things to be refined:
  - Functions
  - Data
- 2 parts :
  - Design refinement
  - Design Verification

Design Refinement

- Done using clear box specification



Incorporating Correctness Verification



How is CV done?

- Formal CV done at each level of refinement
- Generic correction conditions are attached to various structured programming constructs

Examples of CV conditions

- **If a function *f* is expanded into a sequence *g* and *h*, the correctness condition for all input to *f* is**
- • *Does g followed by h do f?*

- **When a function *p* is refined into a conditional of the form, if <*c*> then *q*, else *r*, the correctness condition for all input to *p* is**
- *Whenever condition c is true, does q do p; and whenever c is false, does r do p?*

- **When function *m* is refined as a loop, the correctness conditions for all input to *m* are**
- • *Is termination guaranteed?*
- • *Whenever c is true, does n followed by m do m; and whenever c is false, does skipping the loop still do m?*
- Each time a clear box is refined to the next level of detail, these correctness conditions are applied.

Design Verification

- Does CV for a procedural design.

Procedural Design

Add correctness conditions

Prove the conditions are true for all cases

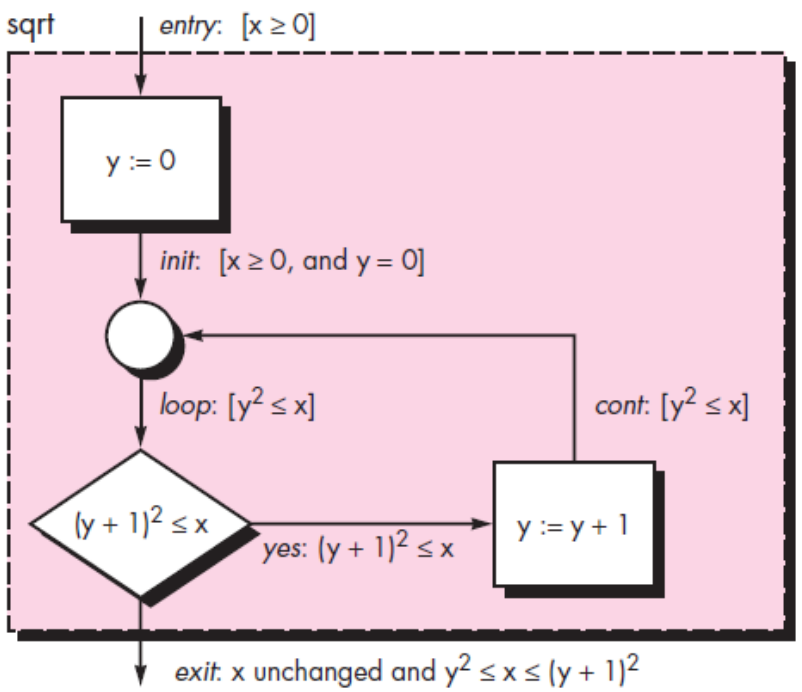
Question

- Design and verify a small program that finds the integer part *y* of a square root of a given integer x.

Solution

- Design and verify a small program that finds the integer part *y* of a square root of a given integer x.
- *Step 1: Show procedural design (flowchart)*
- *Step 2: Add correctness conditions*
- *Step 3: Design Verification (verify the conditions hold true in all cases)*

Final flowchart will look like



CLEANROOM TESTING

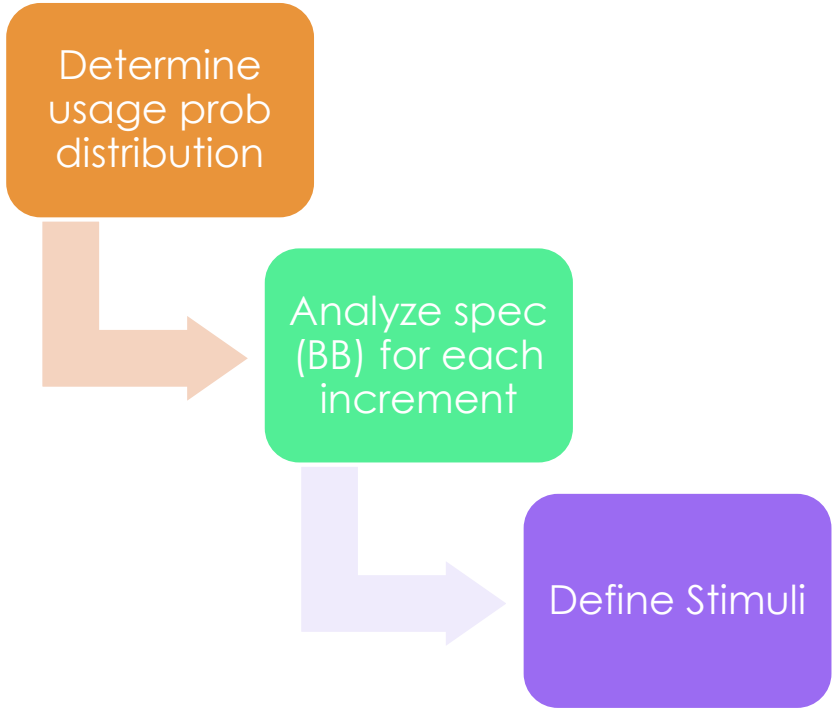
Basics

- Traditional vs Cleanroom Approach
- 2 parts:
  - Statistical Use Testing
  - Certification

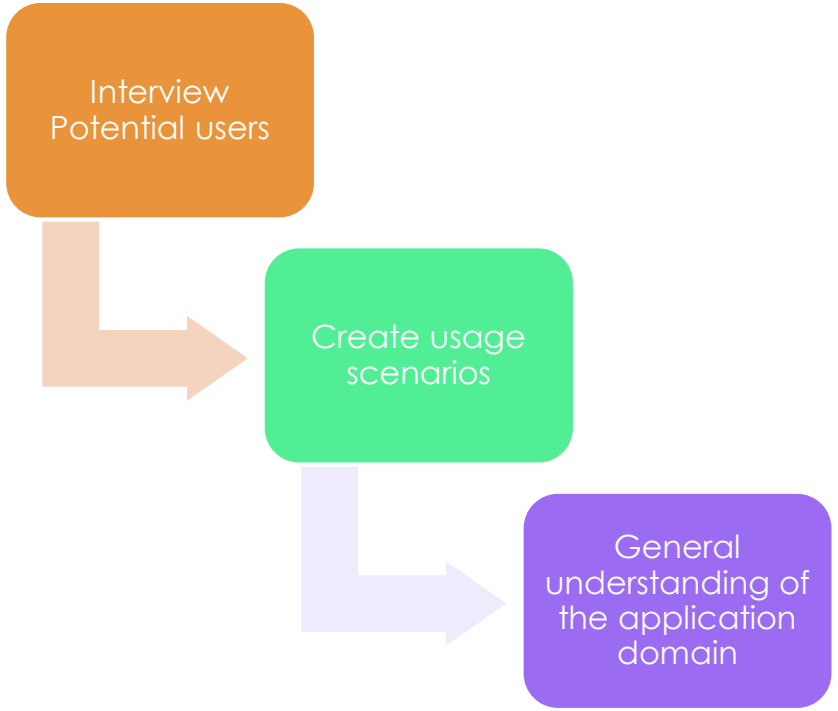
Statistical Use Testing

- What is it?
  - Testing as per intended use by users
  - Why statistical?

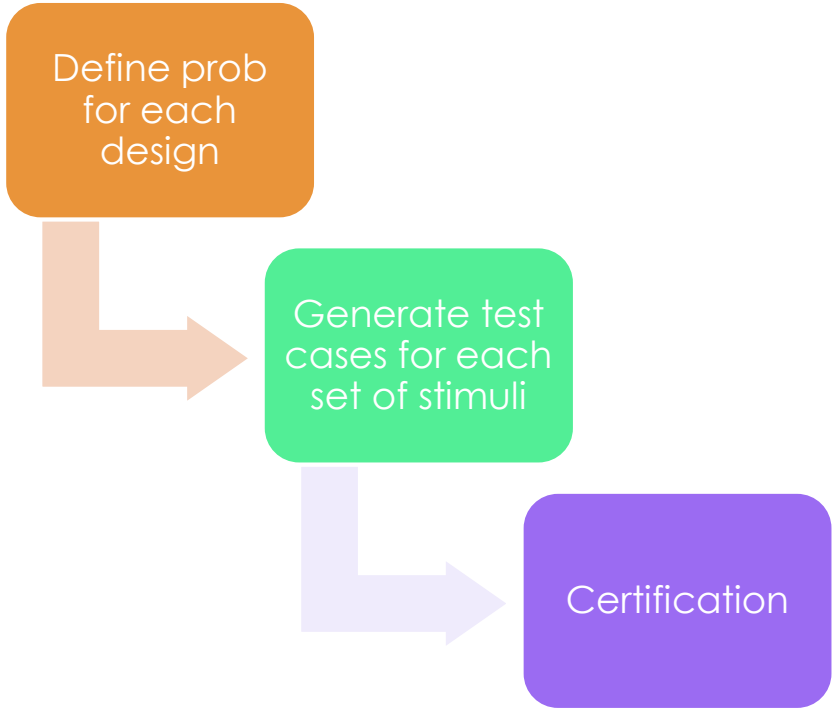
How is it done?



How is it done?



How is it done?



Certification

- Specifies reliability
- Uses MTTF
- Advantages:
  - Reuse
  - Each component will have a certified reliability

Certification Creates three models:

- Sampling Model
- Component Model
- Certification Model

The Certification Process