National Institute of
Standards and Technology
U.S. Department of Commerce

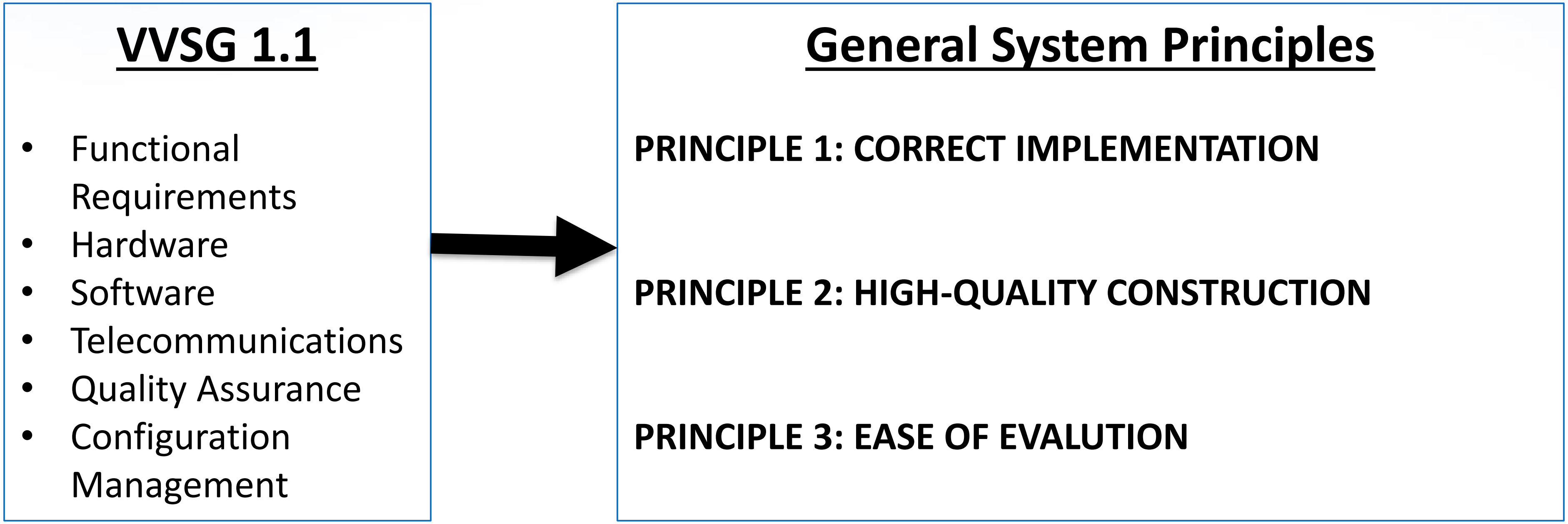
General Principles for VVSG 2.0

Benjamin Long, NIST

TGDC Meeting

February 13/14, 2017

Draft Principles for the Rest of the Standard



VVSG 1.1

- Functional Requirements
- Hardware
- Software
- Telecommunications
- Quality Assurance
- Configuration Management

General System Principles

PRINCIPLE 1: CORRECT IMPLEMENTATION

PRINCIPLE 2: HIGH-QUALITY CONSTRUCTION

PRINCIPLE 3: EASE OF EVALUTION

Correct Implementation

PRINCIPLE 1: CORRECT IMPLEMENTATION: Completely and accurately support election processes.

- **GUIDELINE 1.1: Across entire election process.**
  - **Functionality** – Support entire **voting process and voting variations**
  - **SW / HW** – Support integrity and maintainability of **election processes and data**
  - **Telecom** – Reliably and accurately transfer **voting-related information**
- **GUIDELINE 1.2: Under realistic operating conditions.**
  - **Functionality** – Ensure processes remain correct during **all operations**
  - **SW / HW** – Correct under **expected work-loads and environmental conditions**
  - **Telecom** – Correct when **transmitting** results remotely
- **GUIDELINE 1.3: Across entire system lifecycle.**
  - **Functionality** – Ensure processes are correct throughout entire lifecycle
  - **SW / HW / Telecom** – Regardless of changes in lifecycle, SW, HW, or telecom
  - **QA/CM** – Tracking process implementations through lifecycle

High-Quality Construction (1)

PRINCIPLE 2: HIGH-QUALITY CONSTRUCTION: Construct to maximize quality.

- **GUIDELINE 2.1: Use trustworthy materials and methods.**
  - **Functionality** – In general, use trustworthy materials, methods, and standards
  - **SW** – Use accepted languages, language tools, coding standards, etc.
  - **HW** – Use standards for climate-related, safety, and environmental hardware testing
  - **Telecom** – Use standardized protocols, interfaces, and technologies
  - **QA/CM** – Use QA/CM methods consistent with recognized quality standards

- **GUIDELINE 2.2: Organize elements and logic of the system meaningfully.**
  - **Functionality** – Support general system properties (e.g., security, accuracy, …)
  - **SW** – Support clear meaningful logic, simple modular organization, robust change
  - **HW/Telecom** – Support essential software operations / data integrity
  - **QA/CM** – Support logical / physical configuration control

High-Quality Construction (2)

- **GUIDELINE 2.3: Handle errors actively and appropriately, recovering from failure gracefully.**
  - **Functionality** – Use robust processing in general (active error handling, graceful recovery)
  - **SW** – Check for known errors; SW error handling; avoid SW single points of failure
  - **HW/Telecom** – Perform appropriate error handling; avoid single points of failure
- **GUIDELINE 2.4: Perform accurately and reliably in intended environments.**
  - **Functionality** – Support reliable election processing in general.
  - **SW** – Ensure is free of well-known security vulns.; protected against threats (SW, env.)
  - **HW** – Ensure reliable performance and pervasive accuracy, integrity, durability, safety
  - **Telecom** – Satisfy performance criteria for accuracy, durability, reliability, and integrity

High-Quality Construction (3)

- **GUIDELINE 2.5: Support auxiliary aims and processes (e.g., auditing, testing, …).**
  - **Functionality** – Support auxiliary functions for operations / transparency (auditing, testing, …)
  - **SW** – Provide software and data support
  - **HW** – Provide hardware and data support
  - **Telecom** – Provide telecom-specific and data support
  - **QA/CM** – Track system configurations across its lifecycle

Ease of Evaluation

PRINCIPLE 3: EASE OF EVALUTION: Support clear evaluation by reviewers.

- **GUIDELINE 3.1: Clearly identify all essential elements of system in implemented systems.**
  - **Functionality** – Ensure unique election/auxiliary processes/functions are **clearly identifiable**
  - **SW** – Ensure are clearly identifiable in **software**
  - **HW** – Ensure are clearly identifiable in **hardware**
  - **Telecom** – Ensure are clearly identifiable in **telecom-components**
  - **QA/CM** – Track ability to clearly identify unique processes and functions

- **GUIDELINE 3.2: Clearly distinguish correct/incorrect configurations in implemented systems.**
  - **Functionality** – Ensure correct processes / functions are **clearly distinguishable** from incorrect
  - **SW** – Ensure are clearly distinguishable in **software**
  - **HW** – Ensure are clearly distinguishable in **hardware**
  - **Telecom** – Ensure are clearly distinguishable in **telecom-components**
  - **QA/CM** – Track ability to clearly distinguish correct from incorrect processes and functions

Initial Gap Analysis

Observations	Considerations / Questions
Software • Expanded languages + execution environments • Basis for review: style, substance	**Goal:** Meaningfully verify logic is correct • Appropriate coverage, given scope? • Most appropriate verification mechanisms?
Hardware/Telecom • MIL-STDs • Increased usage of COTS • New form-factors and configurations • Increased forms of inter-connection/communication	**Goal:** Meaningfully verify reliable, accurate, realistic election workloads • Workload characterization methods? • Acceptable ranges of performance for COTS? • Best approaches for effectively and meaningfully testing new COTS configurations? • Evaluation of new forms of inter-connection?
QA/CM • Same quality standards/conventions • Changing environments for development and evaluation	**Goal:** Meaningfully verify manufacturing processes reliable/reproducible • Best means for evaluating production process quality transparently and explicitly?
TDP • Documentation to support evaluation	**Goal:** Have all information necessary for high-quality evaluations • Best means to explicitly support evaluations?
Testing • Need for greater coverage and consistency	**Goal:** Meaningfully interpret observable evidence of required features • Best means for ensuring accuracy, testability, and consistency of testing? • Across tests and testing institutions? • Appropriate testing granularity?

Discussion?