General Principles & Guidelines

Benjamin Long, NIST
benjamin.long@nist.gov

Principles

High Quality Design

High Quality Implementation

Design & Implementation Considerations

HIGH QUALITY DESIGN

- Is domain-specific
- Is organized around accurate election process specifications
- Focuses on preserving correct election processes in implementations
- Ensures designs can support clear evaluations in general

HIGH QUALITY IMPLEMENTATION

- Is about applying best-practices and high-quality engineering to create election technology
- Is organized around construction and reliability of election technology implementations

PRINCIPLE: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

GUIDELINES

- The voting system is designed using commonly-accepted election process specifications.
- The voting system is designed to function correctly under all realistic operating conditions.
- Voting system design supports evaluation methods enabling testers to clearly and easily distinguish systems that correctly implement specified properties from those that do not.

High Quality Design (1)

The voting system is designed to accurately, completely, and robustly carry out election processes.

GUIDELINE

The voting system is designed using commonly-accepted election process specifications.

- **Functionality** – Support entire **voting process** **and** *appropriate* **voting variations**
- **SW / HW** – Support integrity and maintainability of **election processes and data**
- **Telecom** – Reliably and accurately transfer **voting-related information**

High Quality Design (2)

The voting system is designed to accurately, completely, and robustly carry out election processes.

GUIDELINE

The voting system is designed to function correctly under all realistic operating conditions.

- **Functionality** – Ensure processes remain correct during **all operations**
- **SW / HW** – Correct under **expected work-loads** encountered in realistic elections
- **Telecom** – Correct when **transmitting** results remotely

High Quality Design (3)

The voting system is designed to accurately, completely, and robustly carry out election processes.

GUIDELINE

Voting system design supports evaluation methods enabling testers to clearly and easily distinguish systems that correctly implement specified properties from those that do not.

- **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

PRINCIPLE: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

GUIDELINES

- The voting system is implemented using trustworthy materials and methods.
- The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters and poll workers, including those with and without disabilities.
- Voting system logic is clear, meaningful, and well-structured.
- Voting system structure is modular, scalable, and robust.
- The voting system supports system processes and data with integrity.
- The voting system handles errors robustly and gracefully recovers from failure.
- The voting system performs reliably in intended environments.

High Quality Implementation (1)

The voting system is implemented using high quality best practices.

GUIDELINE

The voting system is implemented using 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 HW testing
- **Telecom** – Use standardized protocols, interfaces, and technologies
- **QA/CM** – Use QA/CM methods consistent with recognized quality standards

High Quality Implementation (2)

The voting system is implemented using high quality best practices.

GUIDELINE

The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters and poll workers, including those with and without disabilities.

- **Functionality** – Support general system properties (accessibility, usability)
- **SW/HW/Telecom** – architecture and components support application of best practices to
  - ensure representative users can meaningfully, easily, accurately, and safely perform necessary tasks using the system

High Quality Implementation (3)

The voting system is implemented using high quality best practices.

GUIDELINE

Voting system logic is clear, meaningful, and well-structured.

- **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 Implementation (4)

The voting system is implemented using high quality best practices.

GUIDELINE

Voting system structure is modular, scalable, and robust.

- **Functionality** – Support general system properties (e.g., security, accuracy, …)
- **SW/HW/Telecom** – architecture and components support
  - simple modular organization
  - scalability to new data formats
  - stable updates in software and hardware
  - sufficient resources for anticipated volume, scale, and complexity faced by system processes and data
- **QA/CM** – Support configuration control over enterprise architecture

High Quality Implementation (5)

The voting system is implemented using high quality best practices.

GUIDELINE

The voting system supports system processes and data with integrity.

- **Functionality** – Support error detection and correction methods in general processing
- **SW/HW/Telecom –**
  - avoid errors incompatible with election process accuracy
  - support error detection/correction methods in data storage/transmission
  - support built-in measurement, self-test, and diagnostic methods
- **QA/CM** –
  - Support logical/physical configuration control over data storage media & archives

High Quality Implementation (6)

The voting system is implemented using high quality best practices.

GUIDELINE

The voting system handles errors robustly and gracefully recovers from failure.

- **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

High Quality Implementation (7)

The voting system is implemented using high quality best practices.

GUIDELINE

The voting system performs reliably in intended environments.

In intended environments wherein a system is stored, transferred, and used **AND**
Under environmental conditions – temperature, humidity, vibration, shock, electro-magnetic, or other relevant stressors…

- **Functionality** – Ensure all processes remain correct
- **SW** – Ensure logic and data remain correct
- **HW/Telecom** –
  - ensure reliable performance
  - ensure pervasive accuracy, durability, reliability, structural & operational integrity, safety

Questions?

Many thanks to the NIST team for their time and efforts.