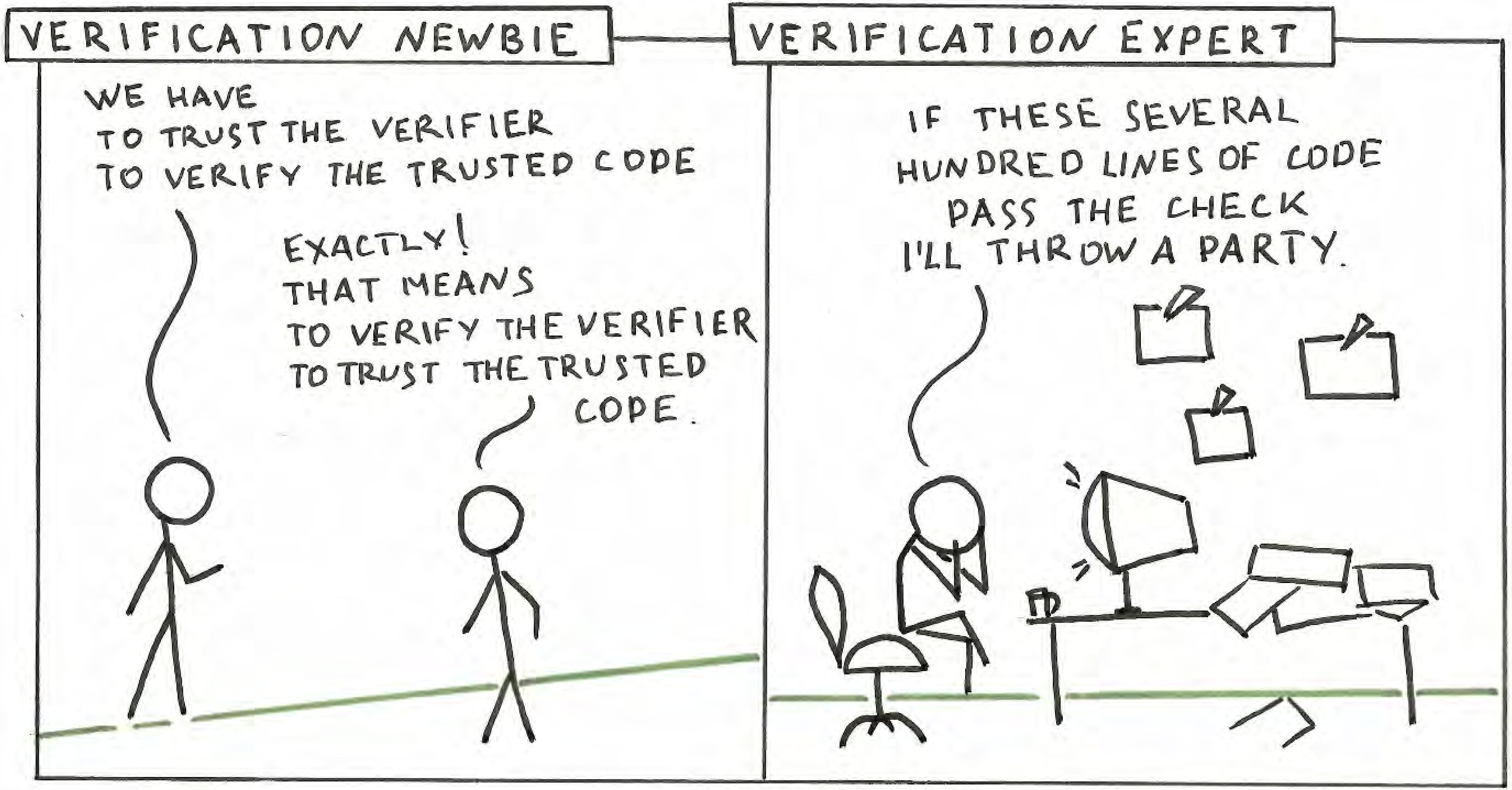
Using IEEE 1012 for Reviews of FPGA-Based Equipment

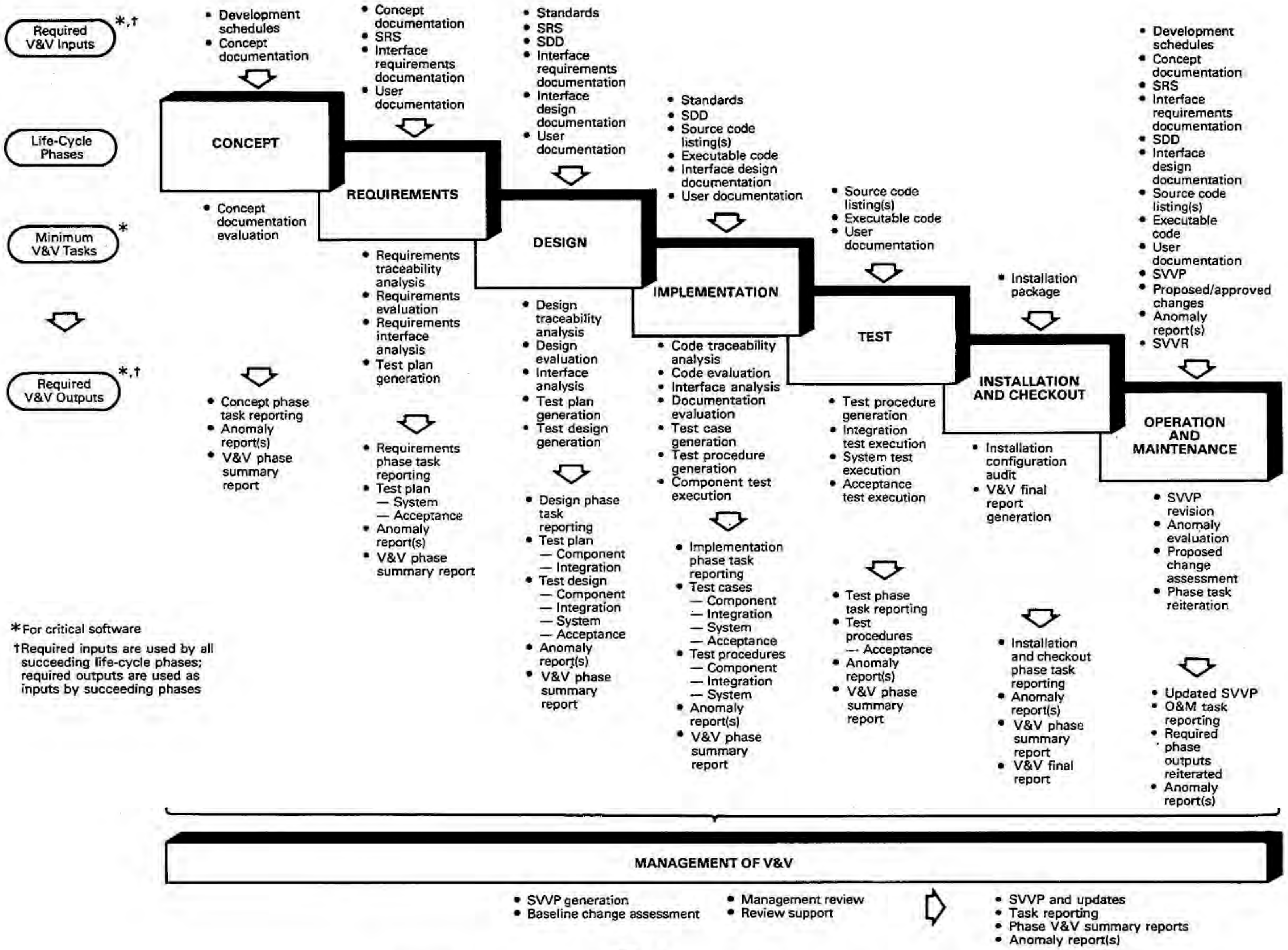
By: Richard Stattel USNRC


VERIFICATION NEWBIE
WE HAVE TO TRUST THE VERIFIER TO VERIFY THE TRUSTED CODE
EXACTLY! THAT MEANS TO VERIFY THE VERIFIER TO TRUST THE TRUSTED CODE.
VERIFICATION EXPERT
IF THESE SEVERAL HUNDRED LINES OF CODE PASS THE CHECK I'LL THROW A PARTY.

IEEE 1012 Concepts and Issues

- SIL Level - Graded Approach to V&V
- Software Criticality Emphasis
- Processes Oriented Guidance
- Example SIL Levels and V&V Activities Included

- Regulatory Endorsement Adaptations
- Hardware and System Processes Introduced in Later Revisions



CONCEPT

- Development schedules
- Concept documentation

- Concept documentation evaluation

- Concept phase task reporting
- Anomaly report(s)
- V&V phase summary report

REQUIREMENTS

- Concept documentation
- SRS
- Interface requirements documentation
- User documentation

- Requirements traceability analysis
- Requirements evaluation
- Requirements interface analysis
- Test plan generation

- Requirements phase task reporting
- Test plan
  - — System
  - — Acceptance
- Anomaly report(s)
- V&V phase summary report

DESIGN

- Standards
- SRS
- SDD
- Interface requirements documentation
- Interface design documentation
- User documentation

- Design traceability analysis
- Design evaluation
- Interface analysis
- Test plan generation
- Test design generation

- Design phase task reporting
- Test plan
  - — Component
  - — Integration
- Test design
  - — Component
  - — Integration
  - — System
  - — Acceptance
- Anomaly report(s)
- V&V phase summary report

IMPLEMENTATION

- Standards
- SDD
- Source code listing(s)
- Executable code
- Interface design documentation
- User documentation

- Code traceability analysis
- Code evaluation
- Interface analysis
- Documentation evaluation
- Test case generation
- Test procedure generation
- Component test execution

- Implementation phase task reporting
- Test cases
  - — Component
  - — Integration
  - — System
  - — Acceptance
- Test procedures
  - — Component
  - — Integration
  - — System
- Anomaly report(s)
- V&V phase summary report

TEST

- Source code listing(s)
- Executable code
- User documentation

- Test procedure generation
- Integration test execution
- System test execution
- Acceptance test execution

- Test phase task reporting
- Test procedures
  - — Acceptance
- Anomaly report(s)
- V&V phase summary report

INSTALLATION AND CHECKOUT

- Installation package

- Installation configuration audit
- V&V final report generation

- Installation and checkout phase task reporting
- Anomaly report(s)
- V&V phase summary report
- V&V final report

OPERATION AND MAINTENANCE

- Development schedules
- Concept documentation
- SRS
- Interface requirements documentation
- SDD
- Interface design documentation
- Source code listing(s)
- Executable code
- User documentation
- SVVP
- Proposed/approved changes
- Anomaly report(s)
- SVVR

- SVVP revision
- Anomaly evaluation
- Proposed change assessment
- Phase task reiteration

- Updated SVVP
- O&M task reporting
- Required phase outputs reiterated
- Anomaly report(s)

MANAGEMENT OF V&V

- SVVP generation
- Baseline change assessment
- Management review
- Review support

- SVVP and updates
- Task reporting
- Phase V&V summary reports
- Anomaly report(s)

*For critical software

†Required inputs are used by all succeeding life-cycle phases; required outputs are used as inputs by succeeding phases

Fig 1
Software Verification and Validation Plan Overview

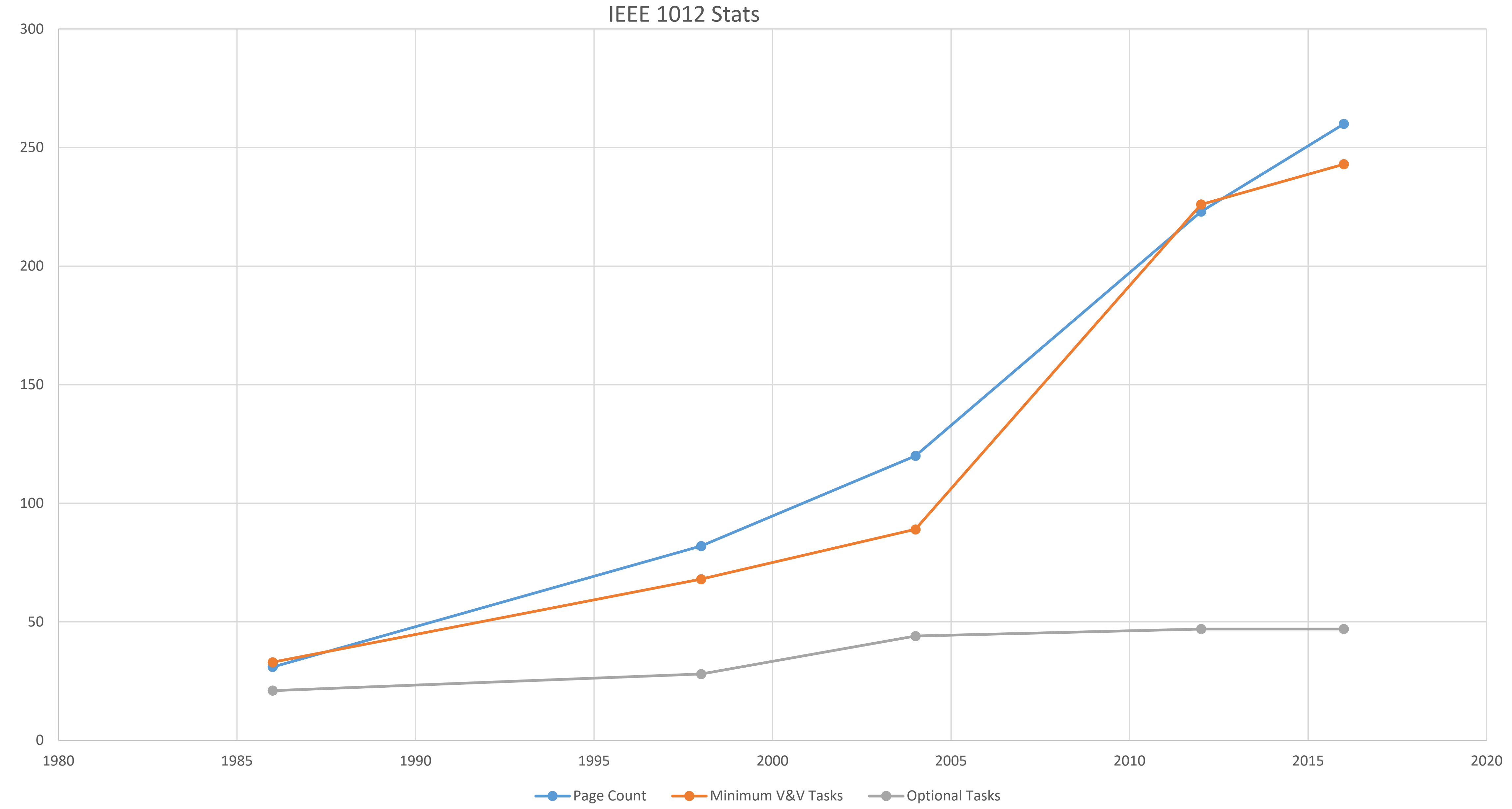
Adaptation

- IEEE 1012 – 1986 Reaffirmed in 1992
  - 31 Pages
  - 33 Minimum V&V Tasks Identified in Table 1
  - 21 Optional Tasks (Table 2)

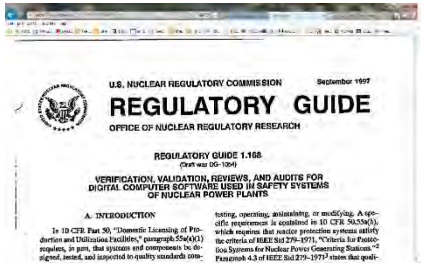
- Revision – 1998
  - Changed from Product base to Process base
  - 82 Pages
  - 68 Minimum Tasks (Table 1)
  - Created new table to align min V&V Tasks to phase (Table 2)
  - 28 Optional Tasks (Table 3 now)

More Adaptation

- IEEE 1012 – 2004 Revision
  - 120 Pages
  - 89 Minimum V&V Tasks Identified in Table 1
  - 44 Optional Tasks (Table 2)
- IEEE 1012-2012 Revision
  - 223 Pages
  - 226 Minimum V&V Tasks
  - 47 Optional Tasks
- IEEE 1012-2016 Revision
  - 260 Pages
  - 243 Minimum V&V Tasks
  - 47 Optional Tasks


IEEE 1012 Stats
300
250
200
150
100
50
0
1980
1985
1990
1995
2000
2005
2010
2015
2020
Page Count
Minimum V&V Tasks
Optional Tasks

Acceptance (From RG 1.168 1997)



U.S. NUCLEAR REGULATORY COMMISSION September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.168
(Draft was DG-1054)

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

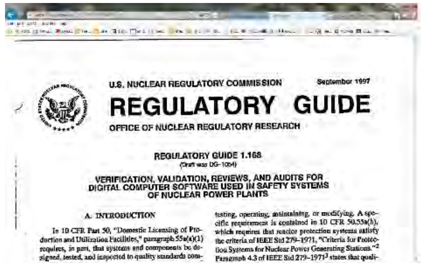
In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety functions to be performed … testing, operating, maintaining, or modifying. A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."[2] Paragraph 4.3 of IEEE Std 279-1971[3] states that quali-

- RG Position

The requirements specified in IEEE Std. 1012-1986 provide an approach that is acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance given in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to the verification and validation of safety system software, subject to the exceptions listed below in Regulatory Positions 1 through 8 and 11.

- Exceptions

Exceptions



U.S. NUCLEAR REGULATORY COMMISSION September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.168
(Draft was DG-1064)

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

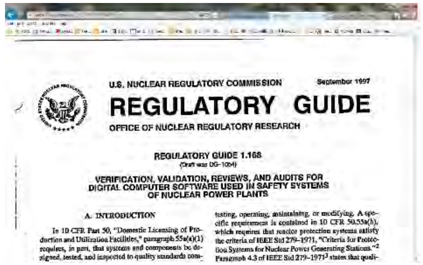
A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards com-

testing, operating, maintaining, or modifying. A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279–1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."[2] Paragraph 4.3 of IEEE Std 279–1971[3] states that quali-

- Critical Software
- Software Reliability
- Independence of Software V&V
- Design Changes
- Conformance of Materials
- Quality Assurance
- Tools for Software Development
- V&V Tasks
- Clarifications

Exceptions



U.S. NUCLEAR REGULATORY COMMISSION September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.168
(Draft was DG-1054)

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

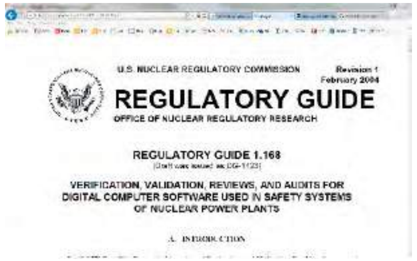
A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards com-

testing, operating, maintaining, or modifying. A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279–1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."[2] Paragraph 4.3 of IEEE Std 279–1971[3] states that quali-

- Critical Software
- Software Reliability
- Independence of Software V&V
- Design Changes
- Conformance of Materials
- Quality Assurance
- Tools for Software Development
- V&V Tasks
- Clarifications

RG 1.168 2004 Revision 1



U.S. NUCLEAR REGULATORY COMMISSION

Revision 1
February 2004

REGULATORY GUIDE
OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.168
(Draft was issued as DG-1123)

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR
DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS
OF NUCLEAR POWER PLANTS

A. INTRODUCTION

IEEE Std 1012-1998 defines a four-level method of quantifying software criticality, in which level 4 is the highest and level 1 the lowest (Clause 4.1). IEEE Std 1012-1998 requires the applicant or licensee either use the method in the standard or define another method and provide a mapping between the applicant's or licensee's method and the method defined in the standard.

Software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Std 1012-1998.

NRC Position SIL Scheme Issue

- NRC Position
  - Software used in nuclear power plant safety systems should be assigned **integrity level 4**

- IEEE 1012 Compliance - Process Basis
  - **Any software integrity level scheme may be used** with this standard.
  - The software integrity level scheme used in this standard is not mandatory, but rather, establishes the minimum V&V tasks for the referenced software integrity scheme.

NRC Position SIL Definition Issue

- NRC Position
    - Software used in nuclear power plant safety systems should be assigned integrity level 4

- SIL 4 Definition (From 2004 Std.)
    - Software element must execute correctly or grave consequences (loss of life, loss of system, economic or social loss) will occur. No mitigation is possible.

- Thus;
    - Failure of Software used in Safety Systems must result in grave consequences without any means of mitigation.

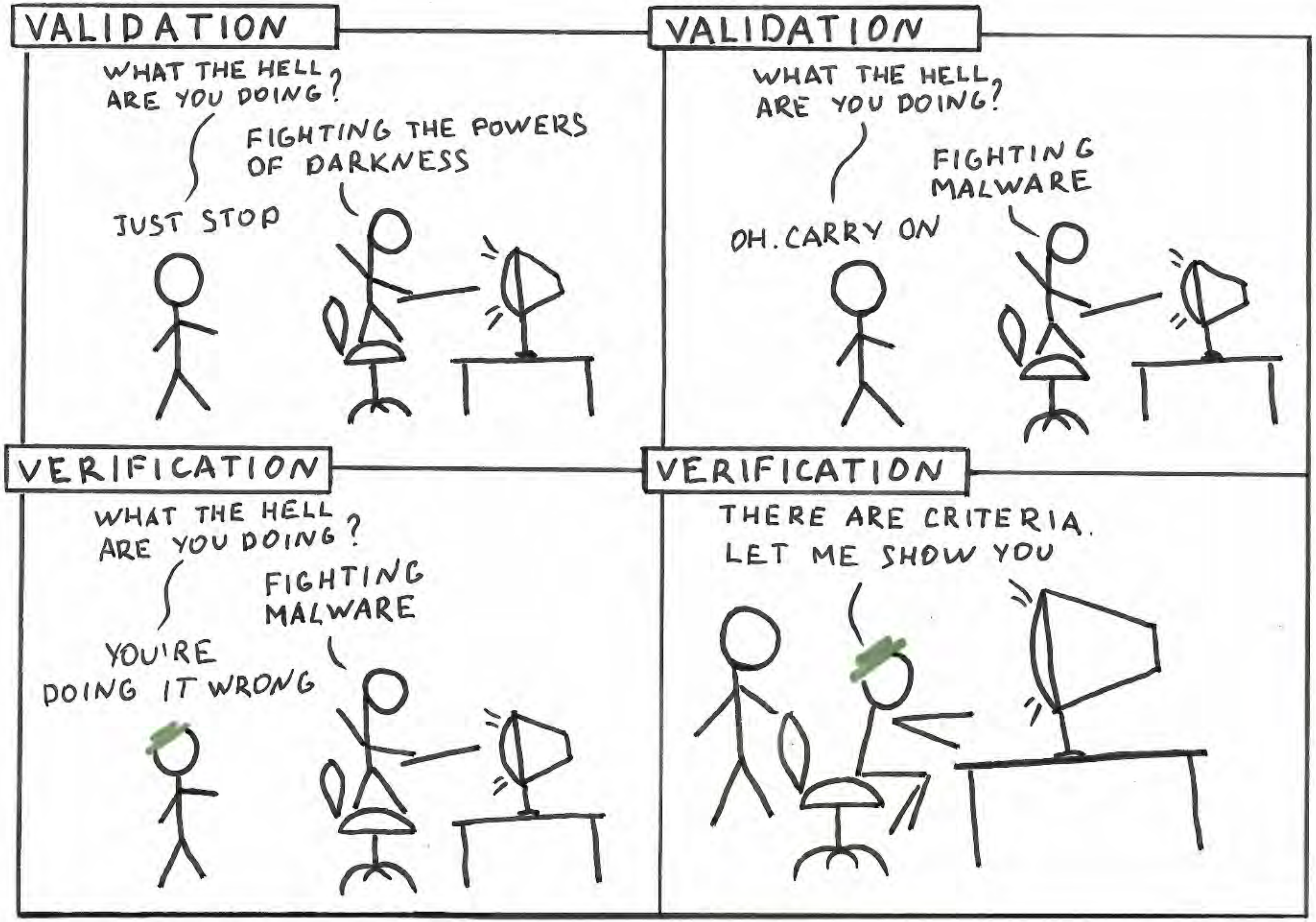
Application

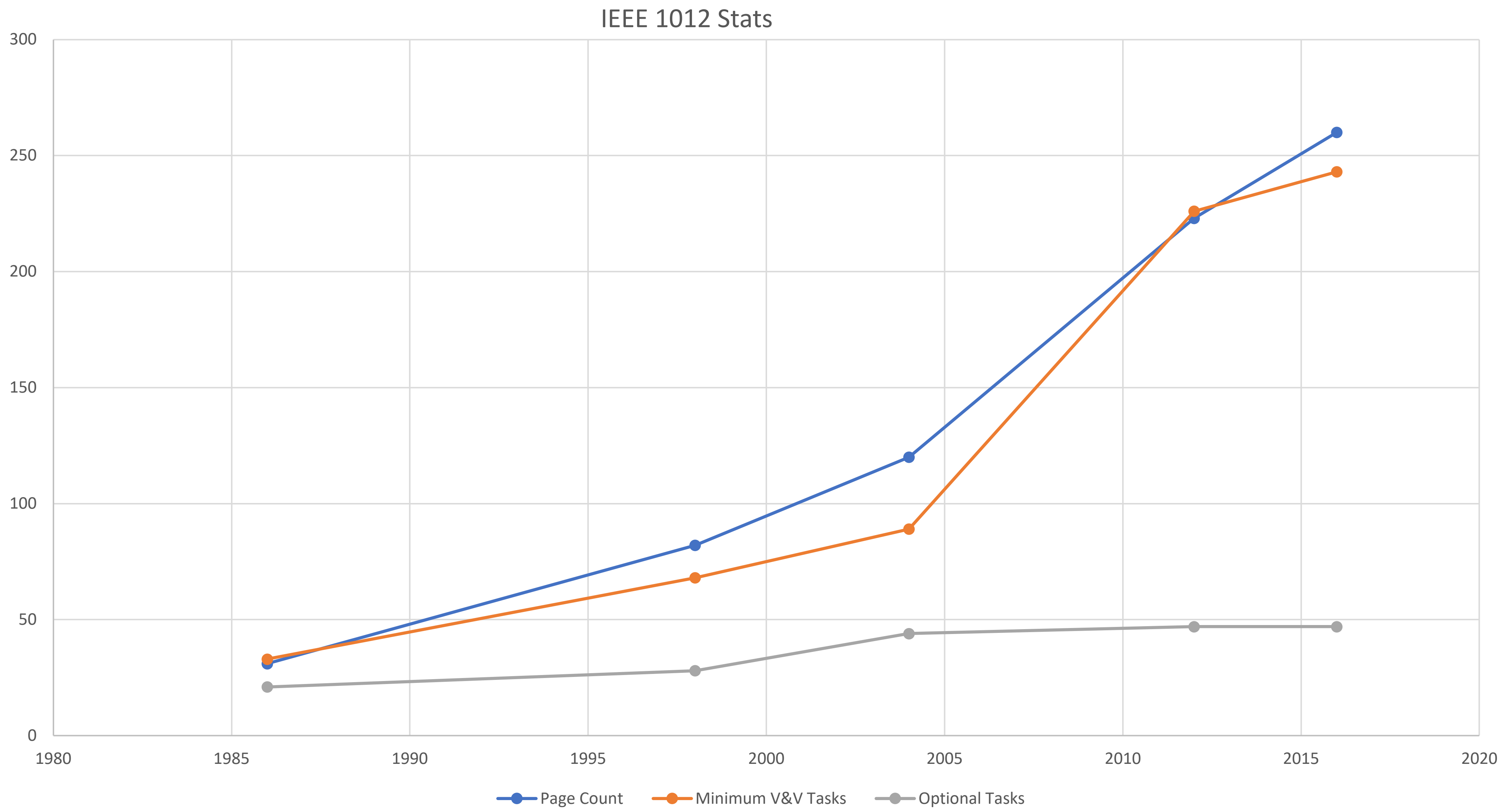
- Applications with Software
  - Eagle 21 RPS Systems
  - Plaform Evaluations
    - Common Q
    - Teleperm TXS
    - Triconics

- FPGA Applicability
  - ALS / NUPAC Platform Evaluations
  - Diablo Canyon
  - FPGA Equivalent Tasks Identified
    - HDL Code = Software Instructions / code
    - Development Tool / Environment is software based and is similar
    - Audit / CM / Test Coverage / Traceability / Criticality / Risk / Hazard analyses Tasks, etc.

Evolution

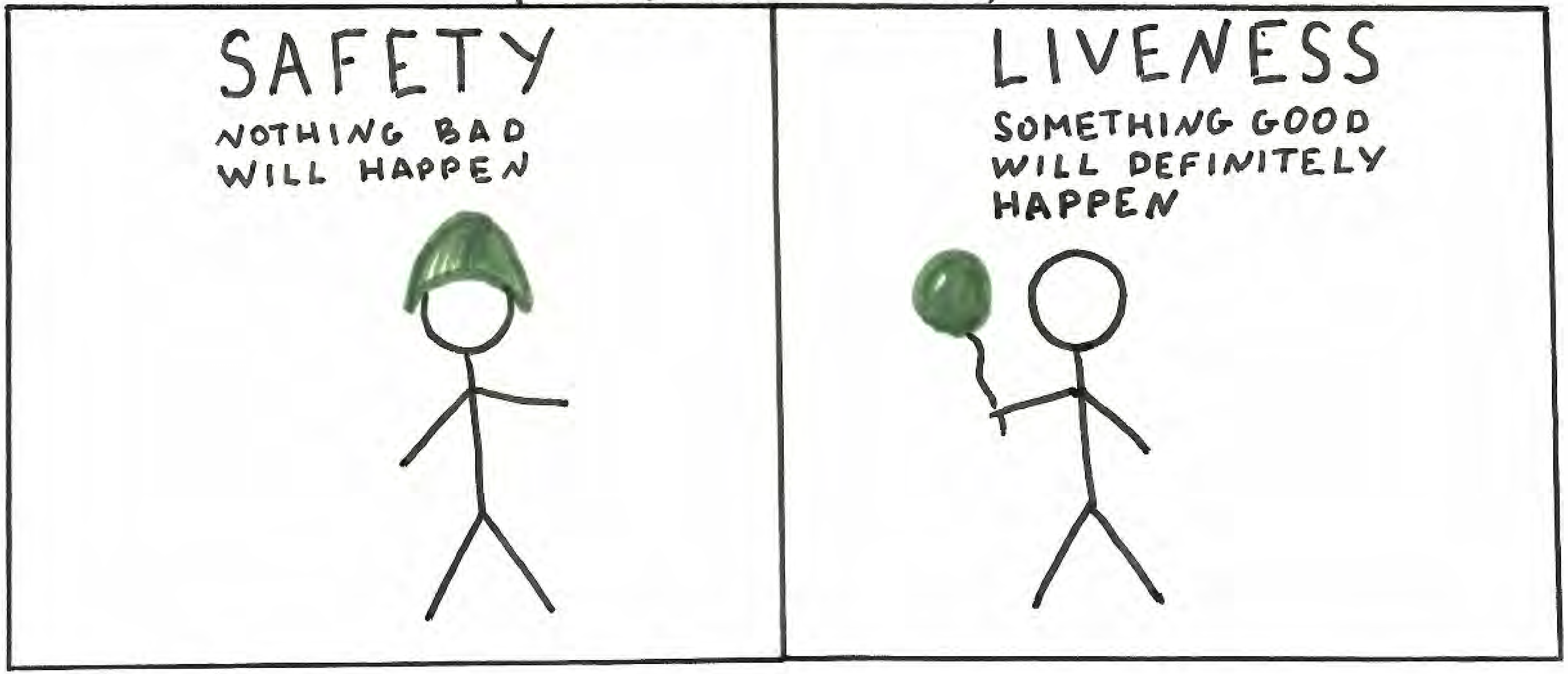
- New IEEE 1012 Versions
  - More V&V Tasks
  - Expanded the scope of the V&V processes to include systems and hardware as well as software
  - New Annexes added to address V&V for Digital System Hardware and Systems
  - Revised to align more completely with the terminology and structure of ISO/IEC/IEEE 15288:2015(E) [B16] and ISO/IEC 12207:2008
  - Minimum V&V tasks for each integrity level.
  - Detailed criteria for V&V tasks


VALIDATION
WHAT THE HELL ARE YOU DOING?
FIGHTING THE POWERS OF DARKNESS
JUST STOP
VALIDATION
WHAT THE HELL ARE YOU DOING?
FIGHTING MALWARE
OH. CARRY ON
VERIFICATION
WHAT THE HELL ARE YOU DOING?
FIGHTING MALWARE
YOU'RE DOING IT WRONG
VERIFICATION
THERE ARE CRITERIA. LET ME SHOW YOU


IEEE 1012 Stats
300
250
200
150
100
50
0
1980
1985
1990
1995
2000
2005
2010
2015
2020
Page Count
Minimum V&V Tasks
Optional Tasks

ALL WE REALLY NEED

(FORMALLY PROVEN)


SAFETY
NOTHING BAD WILL HAPPEN
LIVENESS
SOMETHING GOOD WILL DEFINITELY HAPPEN