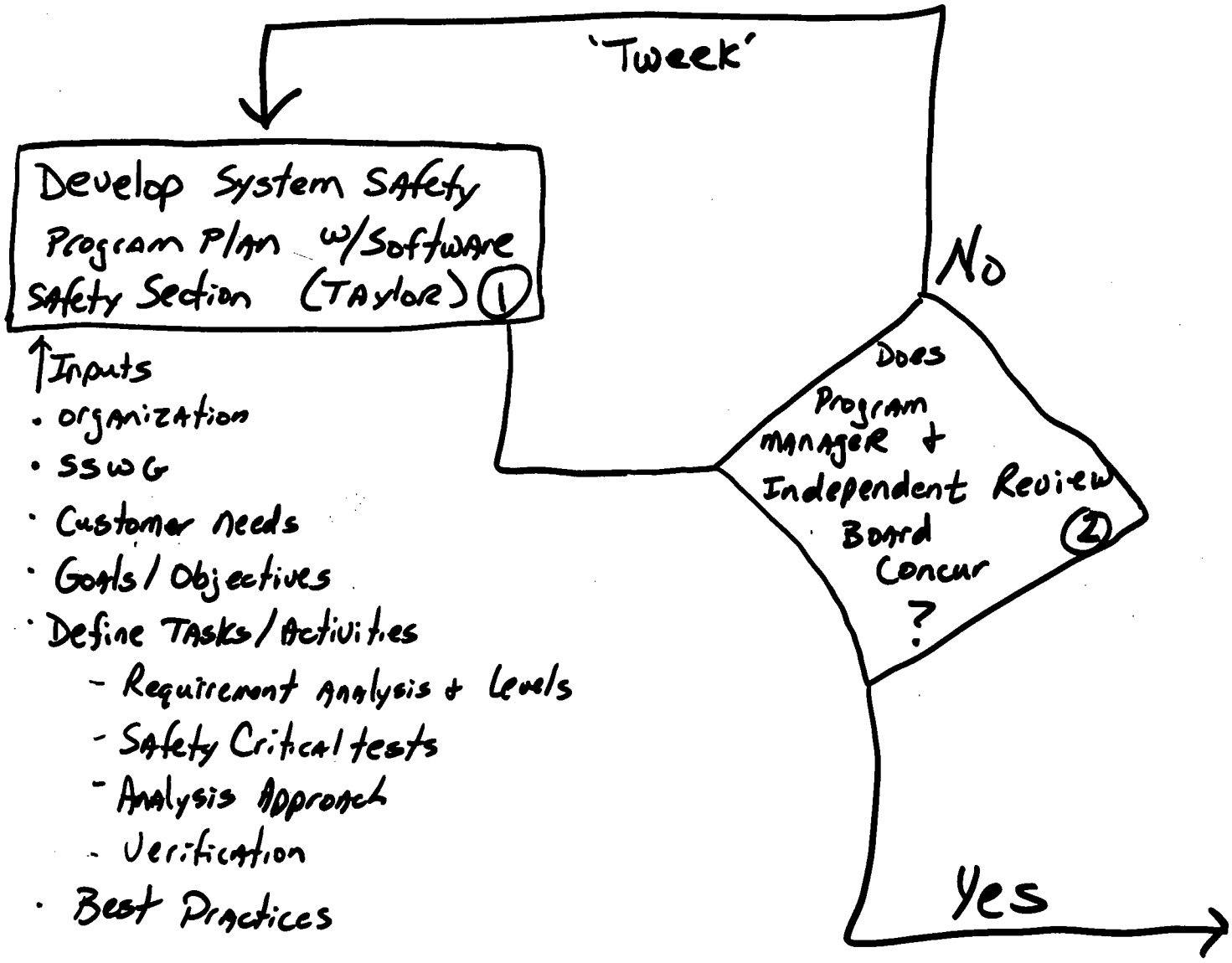
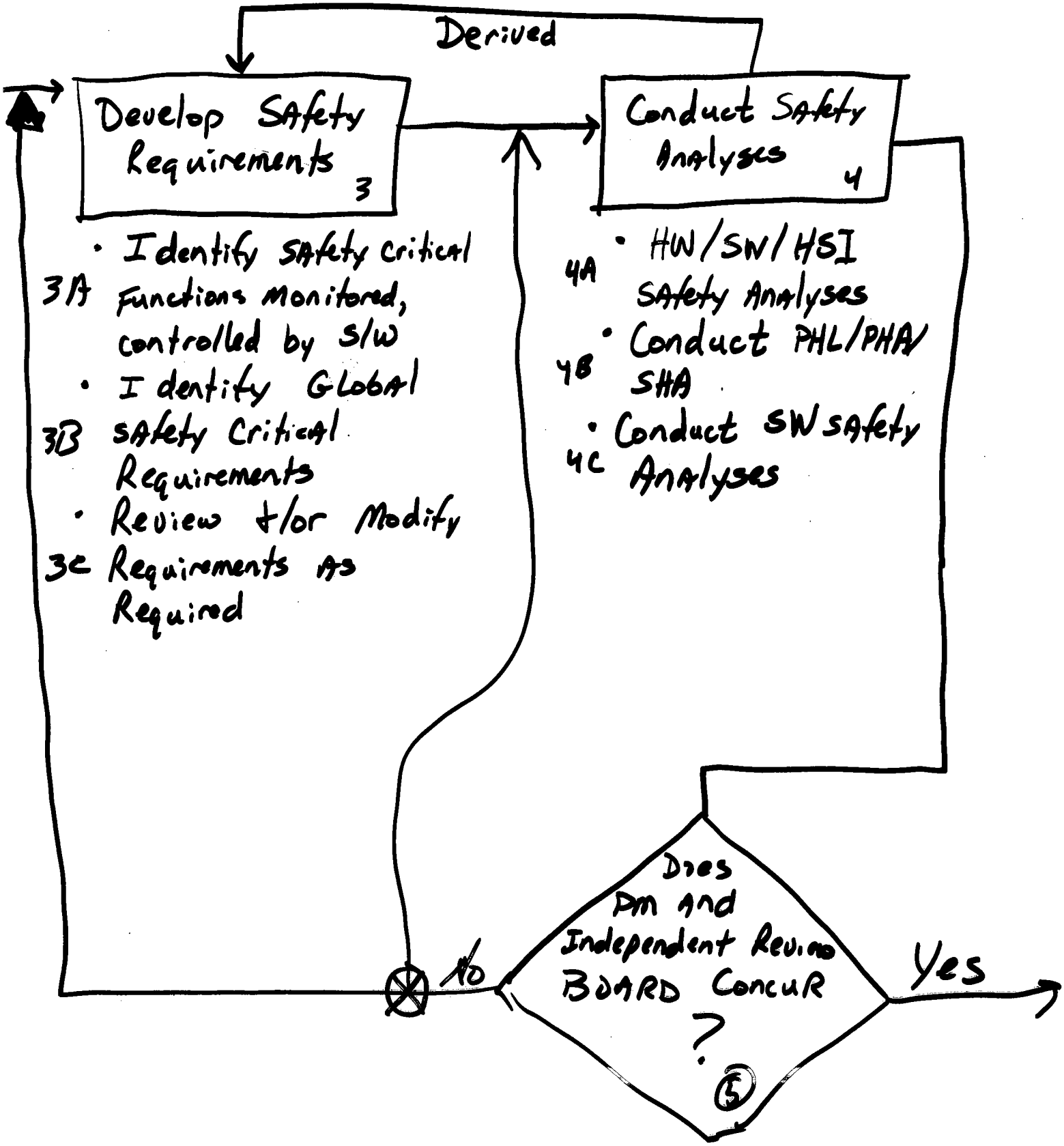
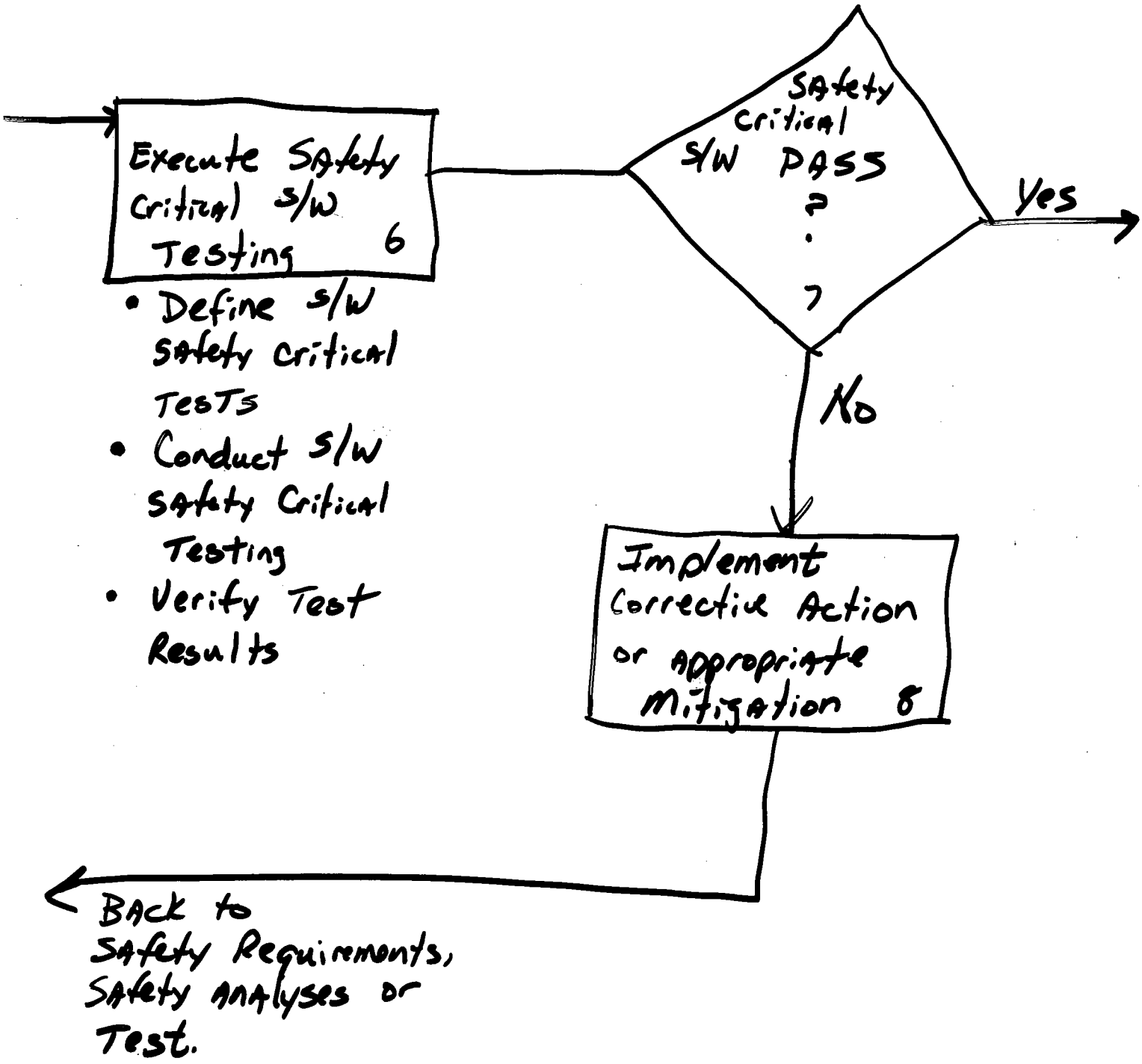


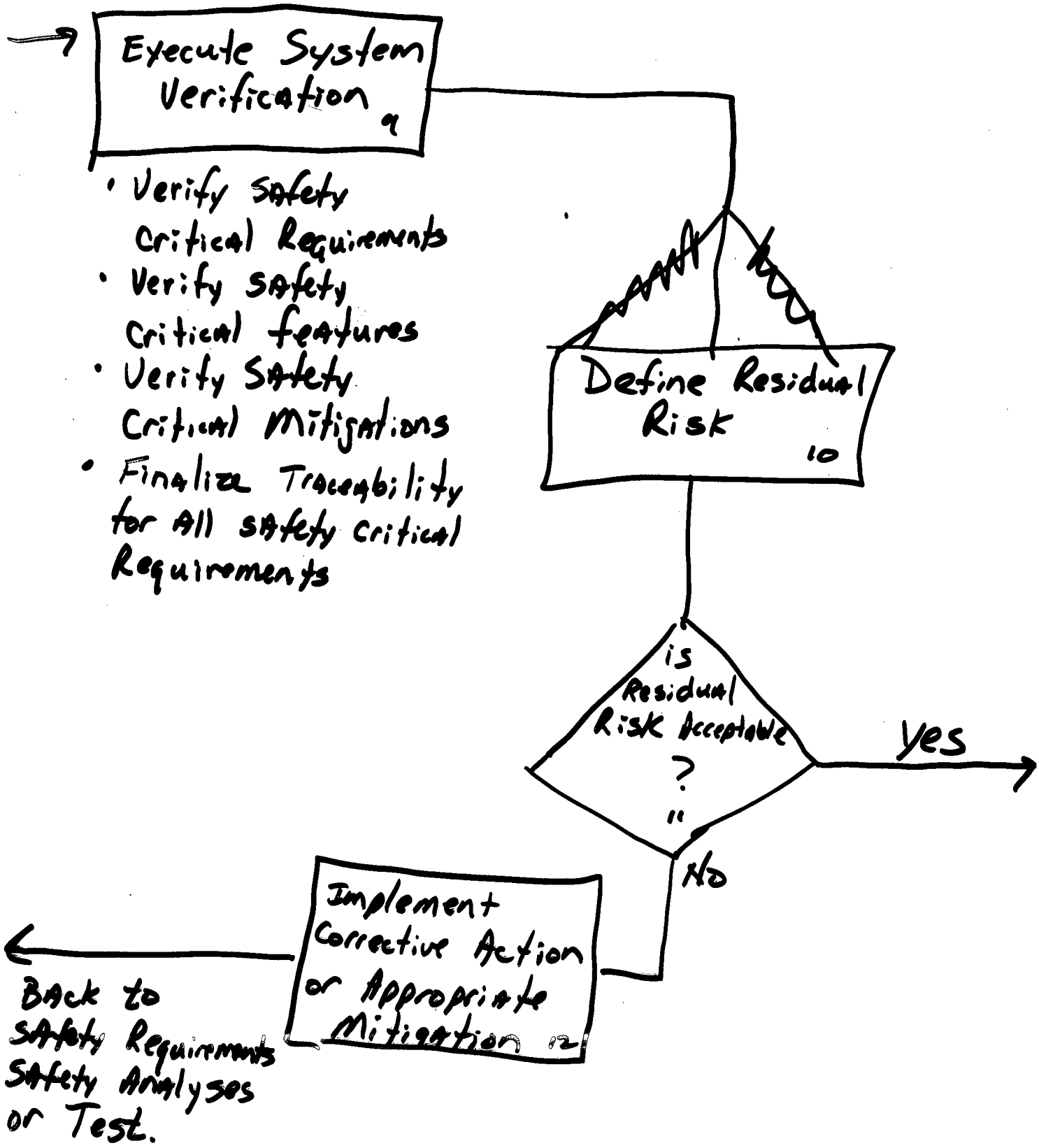
↑Inputs

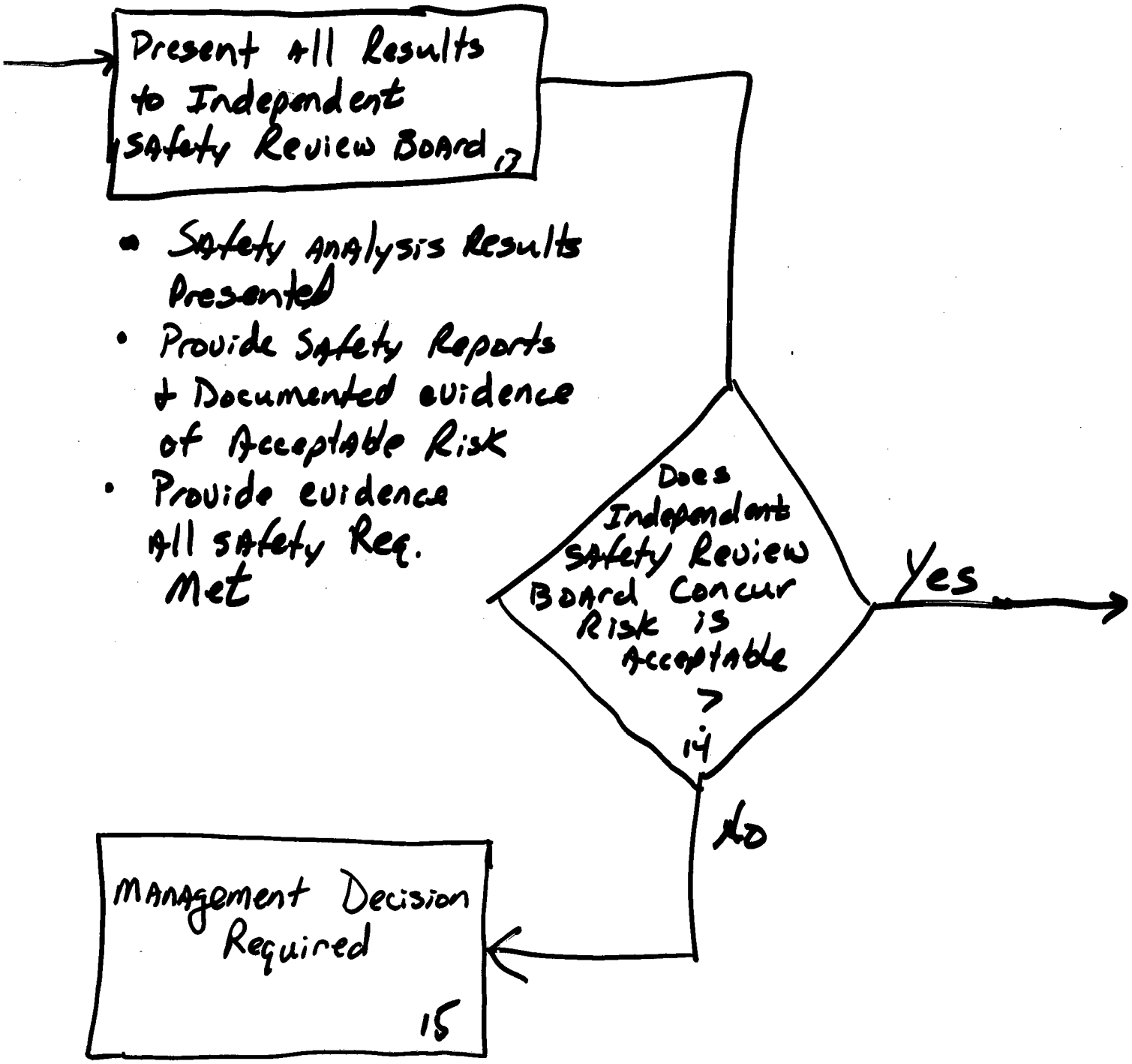
- organization
- SSWG
- Customer needs
- Goals / Objectives
- Define Tasks / Activities
  - Requirement Analysis + Levels
  - Safety Critical tests
  - Analysis Approach
  - Verification
- Best Practices

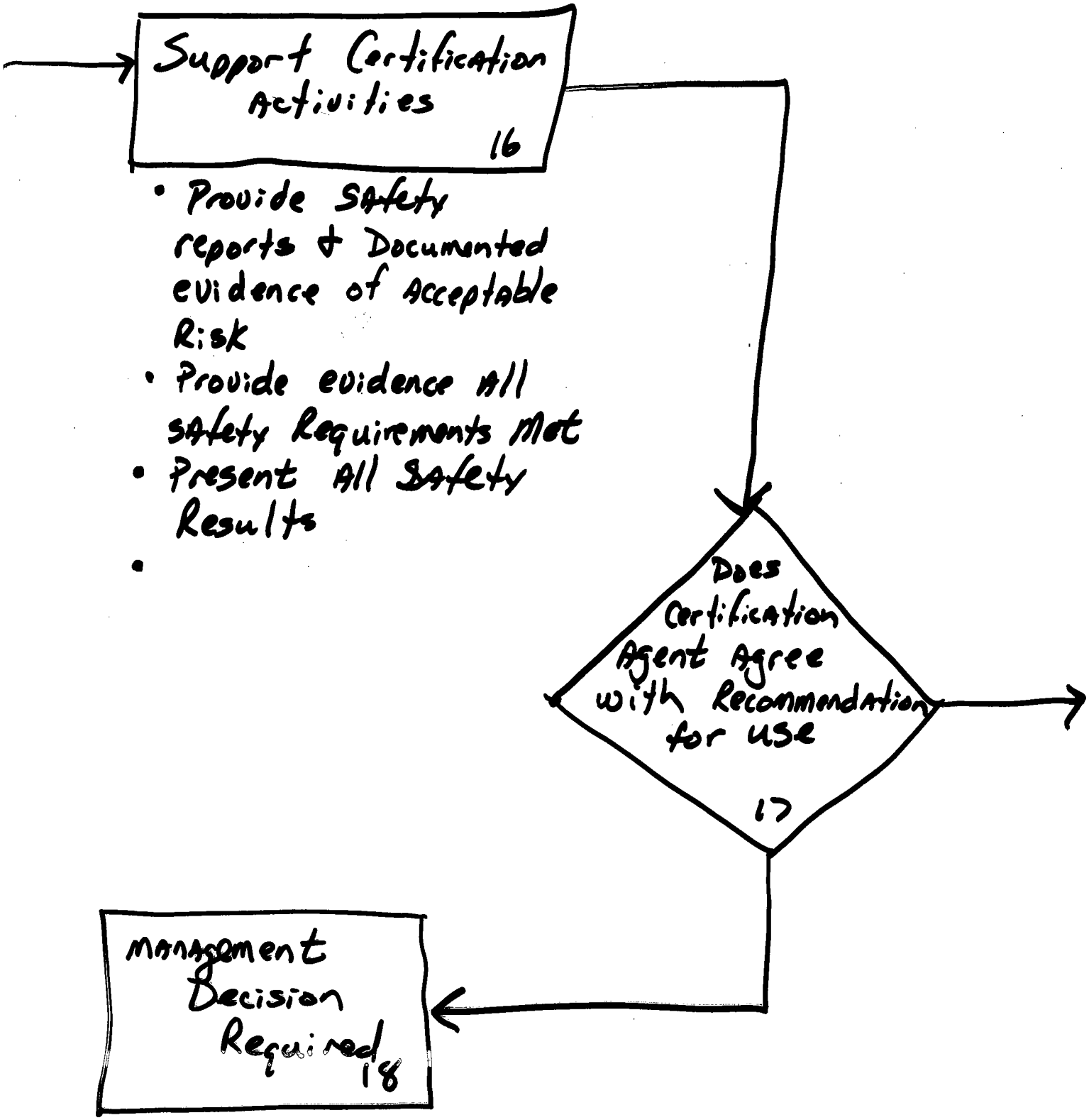

Derived
Develop Safety Requirements 3
Conduct Safety Analyses 4
3A • Identify safety critical Functions monitored, controlled by S/W
3B • Identify Global safety Critical Requirements
3C • Review &/or Modify Requirements as Required
4A • HW/SW/HSI Safety Analyses
4B • Conduct PHL/PHA/SHA
4C • Conduct SW safety Analyses
Does PM and Independent Review BOARD Concur ?
5
No
Yes



- Define S/W Safety Critical Tests
- Conduct S/W Safety Critical Testing
- Verify Test Results


Execute System Verification 9
• Verify Safety Critical Requirements
• Verify Safety Critical features
• Verify Safety Critical Mitigations
• Finalize Traceability for All safety critical Requirements
Define Residual Risk 10
is Residual Risk Acceptable ?
yes
No
Implement Corrective Action or Appropriate Mitigation 12
Back to Safety Requirements Safety Analyses or Test.


Present All Results to Independent Safety Review Board 13
• Safety Analysis Results Presented
• Provide Safety Reports + Documented evidence of Acceptable Risk
• Provide evidence All safety Req. Met
Does Independent Safety Review Board Concur Risk is Acceptable ? 14
Yes
No
Management Decision Required 15


Support Certification Activities
16
• Provide Safety reports & Documented evidence of Acceptable Risk
• Provide evidence All safety Requirements Met
• Present All Safety Results
•
Does Certification Agent Agree with Recommendation for use
17
management Decision Required
18

Maintain Software and Safety Involvement Throughout Life-cycle

19

- Safety involvement in Defect Assessments
- Safety Investigations If necessary
- All ECP's / Proposed changes evaluated
- S/W changes Re-enter process (Safety S/W)