ELECTRIC POWER RESEARCH INSTITUTE

A Utility Standards and Technology Adoption Framework (1023041)

Don Von Dollen
Senior Program Manager, Data Integration & Communications

Grid Interop
December 4, 2012

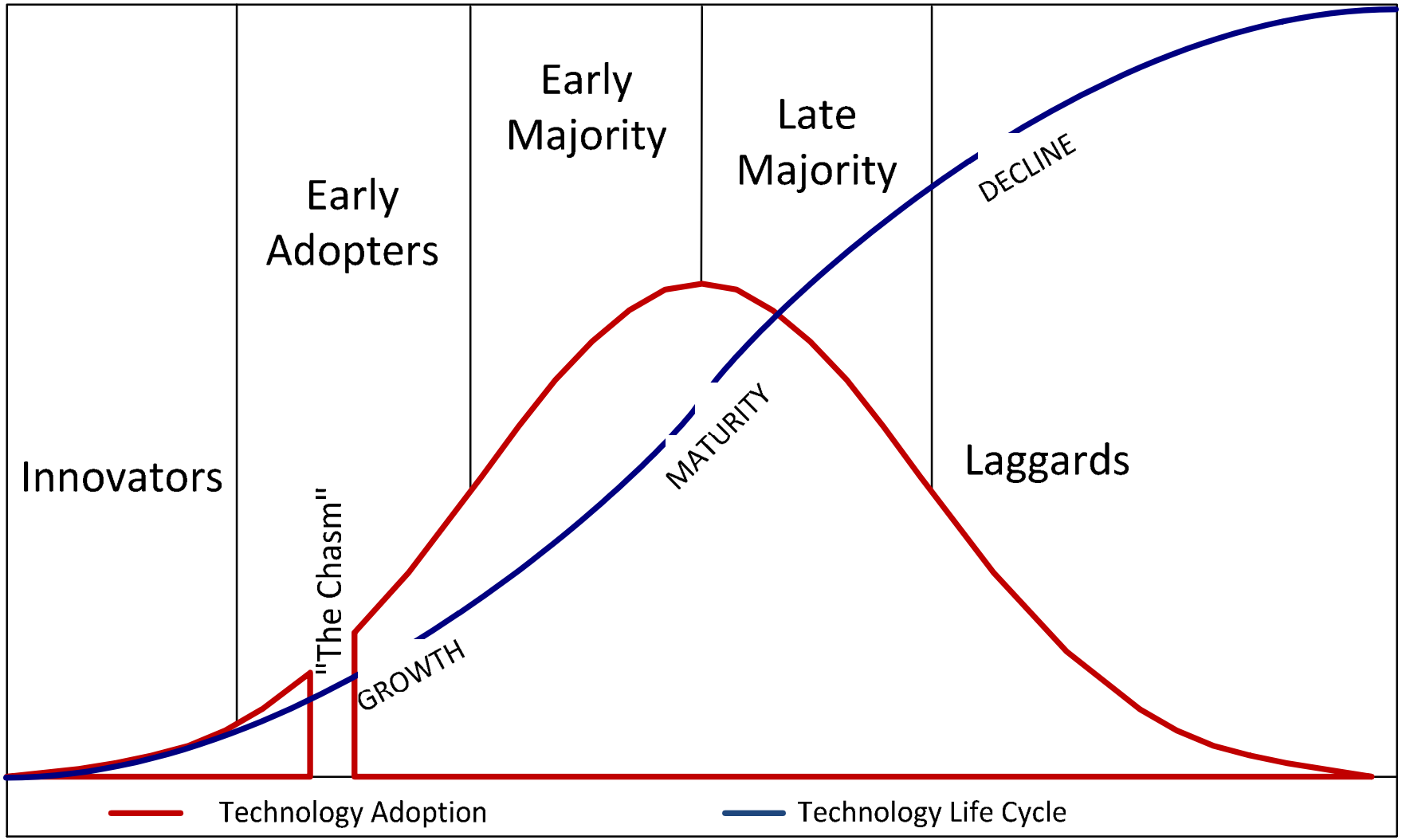
Key Areas for Technology Adoption

1. Clear Business Objective
2. Technology Selection
3. Impact on Existing Infrastructure
4. Ability of Organization to Adapt
5. Method of Implementation
6. Reliability and Security Impacts
7. Testing and Certification
8. Metrics to Evaluate Implementation Effectiveness
9. Cost Recovery and Other Regulatory Issues
10. Business Risk Assessment and Overall Governance
11. Life Cycle Management
12. End of Life

Clear Business Objective

- Business Problem to be solved or opportunity to be explored
- Business and Technical Requirements
- Expected Outcomes
- Costs and benefits with sensitivity analysis to estimate a range of possible outcomes
- Business Value
- Functionality required to achieve specified benefits

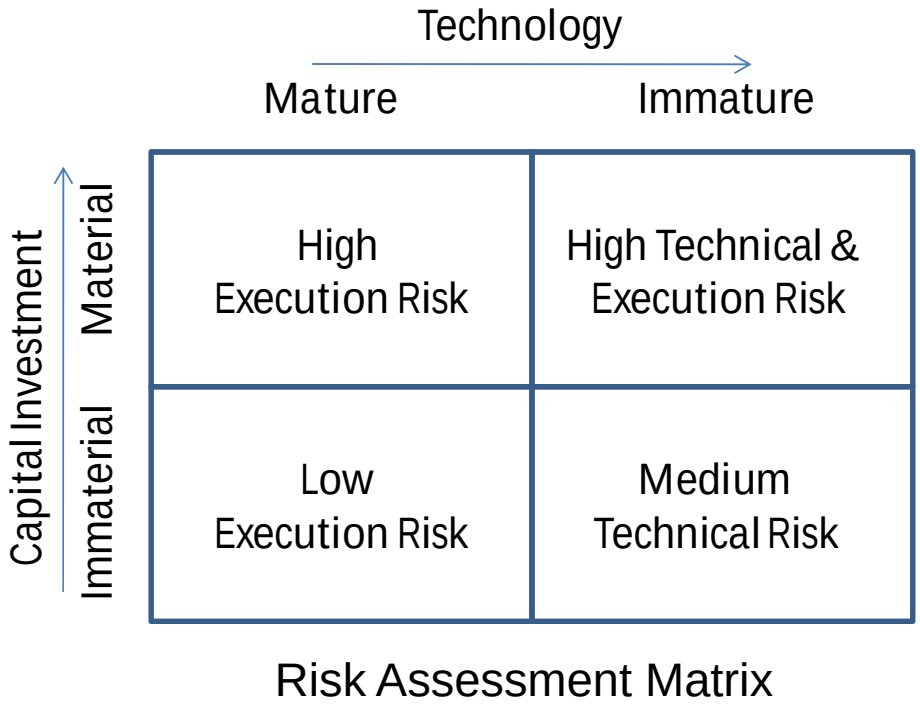
Technology Selection



Technology Adoption and Life Cycle

Impact on Existing Infrastructure

- To assess the impact on existing infrastructure, legacy systems need to be evaluated for potential obsolescence or integration compatibility
- Evaluation techniques and tools can be utilized:
  - Systems interface map
  - Systems lifecycle analysis
  - Configuration Management Database



Risk Assessment Matrix

Ability of Organization to Adapt

- The ability of an organization to adapt will be influenced by:
  - Level of expertise
  - Organizational culture
  - Appropriate training
- Transition techniques and tools can be utilized:
  - Training courses
  - Users Groups
  - Developer Certification

Method of Implementation

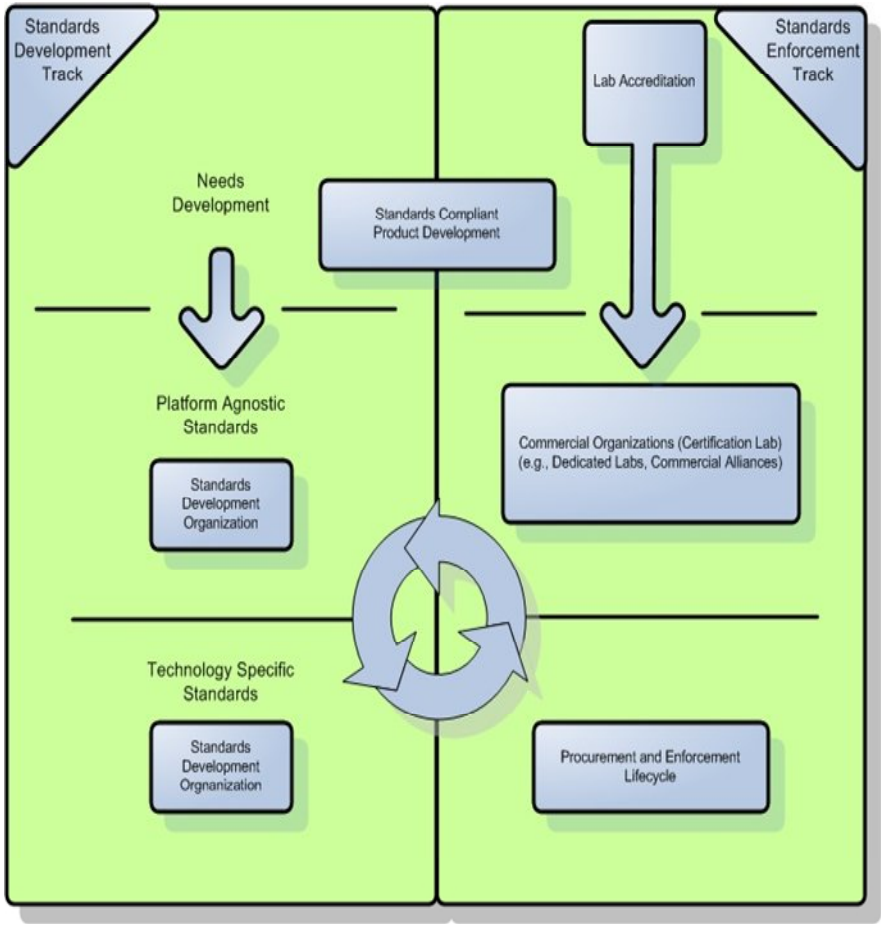
- Implementation strategy may depend on the size and complexity of the system implementation with multiple approaches possible including:
  - R&D
  - Trials
  - Pilots
  - Partial rollouts
  - or full adoption
- The stage-gate approach allows progress to be compared to goals

Reliability and Security Impacts

- System risk is a composite of the risk to each system component
- Security assessments include power system, physical and cyber security aspects
- Combining Security, Disaster Recovery, Availability and Risk Management through continuity management:
  - Determine criticality of systems
  - Assess risks to infrastructure
  - Quantify cost of downtime
  - Determine service level (availability) requirements
  - Assess protection and recovery options based on criticality, risk and cost

Testing and Certification

- Testing ensures compatibility with existing infrastructure and interoperability with other standards based products
- Internal testing capabilities and standards certifications, conformance or compliance certification options should be determined.
- Product demonstrations can be utilized to perform hands-on assessments

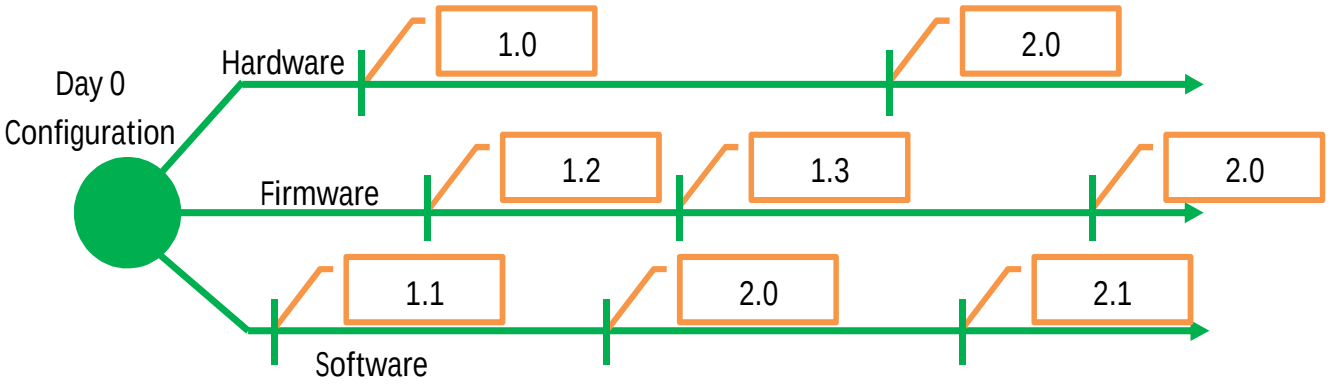


Cost Recovery and Other Regulatory Considerations

- Regulatory engagement and preparation prior to filing an application increases the chances for success.
- Five questions to assess how the smart grid decision will impact the overall stakeholder community:
  - How can the benefits of the project be maximized, while the costs are minimized – what is the best cost/benefit analysis tool to use;
  - How can customer adoption and satisfaction be optimized – what customer education programs are needed and how will they be implemented and financed;
  - How will customer privacy and cyber-security be protected;
  - How will smart grid investments be protected against obsolesce; and
  - What is the plan for future smart grid investment?

Life Cycle Management and End of Life

- Training is more than a one-time occurrence.
- Metrics to monitor system performance should be implemented.
- Continuous improvement involves constant review of opportunities and risks.



Version control of infrastructure components