1. **Overview:** The SVA recommends a multidisciplinary team based approach to conducting a security risk assessment of facilities and operations. The objective of the assessment is to identify hazards, threats, and vulnerabilities faced by a facility as a tool for decision makers to apply appropriate countermeasures to protect the public, workers, national interests, the environment, and the company.

The general approach is to identify critical assets and infrastructure and potential threats, screen out those with low consequences or low target attractiveness to adversaries, and conduct vulnerability analysis on the remaining targets. Finally, risk is evaluated using a risk matrix of consequence and likelihood where likelihood is a function of attractiveness, threat, and vulnerability.

Recommendations are provided for the makeup of the evaluation team and checklists are provided for data collection requirements, countermeasures, and interdependencies. Scenario based examples are provided for several oil and gas segments.

**Applicability**

2. **Target Company:** The methodology is specifically intended for the petroleum and petrochemical industries and is not segment specific (e.g. refineries, pipelines, transportation, etc.). The methodology is general in nature and could be used outside of the oil and gas industry. However, the examples used throughout the document are specific to petroleum and petrochemical companies as well as the checklists.

3. **Scope of Assessment:** The assessment is a general security assessment methodology covering physical and cyber security. The recommended assessment team is broken down into two teams: a full time “core” team and a supporting optional part-time team.

   **The SVA Core Team** members should have the following skill sets and experience:
   - Team leader—knowledge of and experience with the SVA methodology;
   - Security representative—knowledge of facility security procedures, methods and systems;
   - Safety representative—knowledge of potential process hazards, process safety procedures, methods, and systems of the facility;
   - Facility representative—knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures;
   - Operations representative—knowledge of the facility process and equipment operation;
   - Information systems/Automation representative (for cyber security assessment)—knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.
The SVA Optional/Part-time Team members may include the following skill sets and experience:

- Security specialist—knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available;
- Cyber security specialist—knowledge of cyber security practices and technologies;
- Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.;
- Process specialist—knowledge of the process design and operations
- Management—knowledge of business management practices, goals, budgets, plans, and other management systems.

4. **Target Audience for Results:** The result of the assessment is recommended to be summarized in a written report that identifies security vulnerabilities and risk reduction recommendations. The target audience of the report is not explicitly stated but it is recommended that a resolution management system be established to resolve the issues.

**Assessment Process Features**

5. **Data Collection Approach:** An extensive data collection process is recommended including the collection of facility and right of way records, system information, operations records, outside support and regulatory issues, site inspections, previous incident reports, and threat intelligence. Appendix A of the methodology provides a list of supporting data that should be provided to the SVA team. With this information in hand, a series of forms and checklists are provided to assess the information.

6. **Results:** For each of the primary elements of the assessment a scale of one to five is typically used in a qualitative manner. For example, threats are rated from one to five with one being very low indicating no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets to five indicating that a credible threat exists against the asset and that the adversary demonstrates capability and intent to launch an attack. A prescreening is used to remove both low consequence assets and low attractiveness assets (thus low threat). Assets that remain are evaluated and a risk ranking matrix is recommended to evaluate the likelihood and severity of an attack. Risk reduction through countermeasure analysis is then recommended.

7. **Support for Ongoing Assessment Program:** The assessment methodology is sufficiently general in nature that it is left to the owner/operator and the assessment team to determine the level of detail and the specific data collection and targets of evaluation. There are no specific mechanisms for additions and trending.

**Deployment Considerations**

8. **Learning curve:** The “core” team leader is recommended to have knowledge and experience with the SVA methodology. However, the assessment methodology does not use complicated algorithms or aggregation methods. Little training is required to understand the approach.
9. **Cost:** The methodology is publicly available and requires no additional tools for application. However, the core team recommendation is for three to five full time staff plus part-time supporting staff. The actual cost will depend on the scope defined for the study and the depth of data collection.

10. **Schedule:** This is not explicitly stated but will clearly depend on a number of variables including commitment by team members, data and record availability, organization size and complexity, and defined scope.

11. **Technical requirements:** Technical requirements are minimal. The ability to read facility drawings, understand logic diagrams, etc. may be required but the methodology does not require significant technical skill.

12. **Installed base:** Unknown.

13. **Vendor support:** The methodology can be applied entirely by inside personnel. However, for deeper assessments outside contractors may be required. For example, if plant personnel are not trained on cyber security and cyber security is included in the scope of the assessment the contracting of a cyber security professional may be required.

[Ed note 9/12/06: Marty noted in his 3/29/06 email transmitting this draft that the specific technical coverage is not included, but that he felt the SVA was not focused on specifics so coverage would be light. (Also the template for that material was in its infancy at the time when Marty developed this draft.) ]