SAND2015-6639C

Systems Engineering and the Design of Arms Control Monitoring Regimes

Sharon DeLand, Jay Brotz, and Peter Marleau
Sandia National Laboratories

To be accepted, monitoring regimes need to satisfy a complex set of objectives arising from multiple stakeholders. These include (1) providing evidence of compliance, (2) detecting and providing evidence of non-compliance, (3) protecting sensitive information that is not relevant to compliance concerns, and (4) minimizing impact to allowed operations. Technical monitoring measures may draw on a variety of technologies with tradeoffs in capability and intrusiveness. An arms control monitoring regime usually operates within a larger international security framework; it may be combined with other regimes to meet a larger purpose. Understanding the interactions in the larger context is important because it may impact prioritization of objectives within the monitoring regime and may also affect the quality of evidence needed to demonstrate compliance.

Systems engineering is an interdisciplinary methodology for designing, implementing and evaluating successful systems. The methodology emphasizes defining stakeholder needs and functionality early in the process, and uses traceability, verification, and validation to ensure that the system meets desired objectives. It provides a common, well-understood system analysis and design process that organizes and queues design decisions. Systems engineering also uses representations of different aspects of the system (e.g., function, action or dynamics, and physical distribution) to capture the full design or architecture of a system. While the full scope of the systems engineering methodology has applicability to the system level approach to arms control, we want to focus on three specific elements: (1) the context diagram, (2) traceability and allocation of requirements, and (3) verification and validation.

The Context Diagram

In systems engineering, the context diagram describes the boundary between the system under consideration and its environment and describes the interactions of the system with other entities including other systems, stakeholders, and organizations. In a system level approach to arms control, a context diagram would, for example, describe the interaction of an overall cooperative monitoring regime with other sources of information in making an overall determination of compliance. It could clarify which questions are addressed with different sources of information and how information is used to resolve concerns. This is notionally shown in Figure 1 below. A series of diagrams (shown notionally in Figure 2) would define how different nuclear arms regimes fit within a broader arms control framework or ultimately tie to national security objectives.

Traceability and Allocation of Requirements

System design begins with a Concept of Operations – a short description of the problem from the stakeholders' perspective(s). Analysis of the CONOPS results in a set of high-level requirements. The first level of design is to define a set of high level system functions (i.e., monitoring functions) and allocate the high-level requirements to those functions. The requirements may be of differing types. Functional requirements specify some aspect of system performance (e.g., count missiles produced at a facility). Non-functional requirements may be constraints (must encrypt data) or describe a system-wide property such as safety or security. The design process (breaking functions down into sub-functions and defining and allocating requirements) can then be iterated down to a level that specifies design choices. At the highest level, the system functions are not implementation specific. However, as detail is developed, it is useful to develop a physical design and define actions and interactions. For a system level

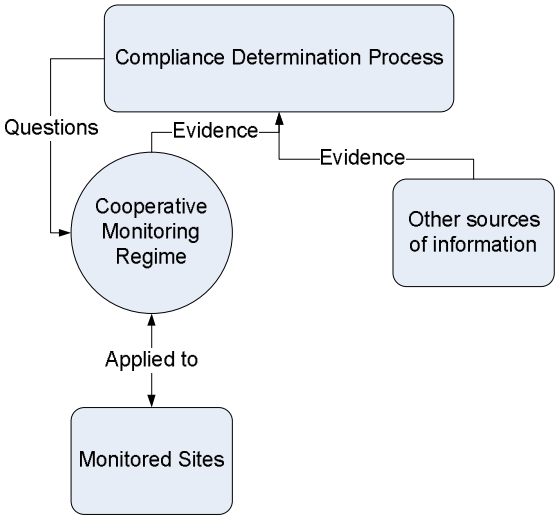

Figure 1: A simplified context diagram for a cooperative monitoring regime

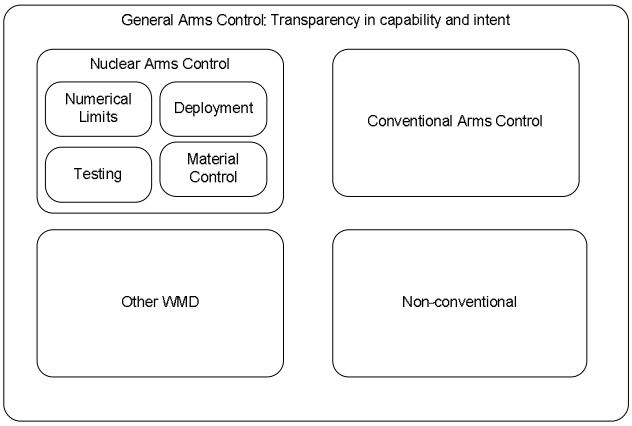

Figure 2: Nuclear Arms Control Regimes in a Broader Context

look at a state enterprise, a high-level physical design could define what facilities are monitored and for what purpose. Lower-level designs begin to address how monitoring occurs at each facility for example. Traceability of requirements from the highest level down to the lowest level provides confidence that the highest level objectives will be met.

Verification and Validation

Verification and validation provide evidence that requirements and objectives have been met. Verification is generally about whether the requirement has been met correctly, validation addresses whether the correct problem has been solved – essentially the correctness and completeness of the requirements. In the context of an arms control regime, verification will test to see whether the regime collected the expected data; validation will address whether or not useful conclusions can be drawn from the data.

Next steps

In the context of system level approaches to arms control, the highest level objectives may not be clearly defined because national security contexts may vary between countries and monitoring regimes are, in the end, the result of detailed negotiations. Nonetheless, there are a number of next steps that the nuclear materials management community could undertake to increase the likelihood that future regimes will better address the information needed to provide confidence and the associated risks. This could include exploration of context diagrams for existing and future regimes in order to understand the range of interactions a regime may need to support. It could also include expanding the context upward to establish traceability to larger security objectives. From the perspective of a technical community, we suggest that this activity is useful insofar as it identifies implicit monitoring objectives that ultimately affect requirements and design decisions.

A second important step would be to outline concepts of operation, high-level requirements, and high-level designs for some subset of monitoring regimes. This activity could start to define common or standard monitoring architectures, for example. Deeper dives into specific regimes could more explicitly connect potential monitoring needs to technology R&D. Stepping back and developing high-level regimes that spanned deployed weapons, non-deployed weapons, material control and R&D for example, would support analysis of the interplay between different regimes in providing confidence. Finally, the community could work together to develop standards for validation of performance of monitoring regimes.