Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Module integration interface for Resilient Cyber Systems

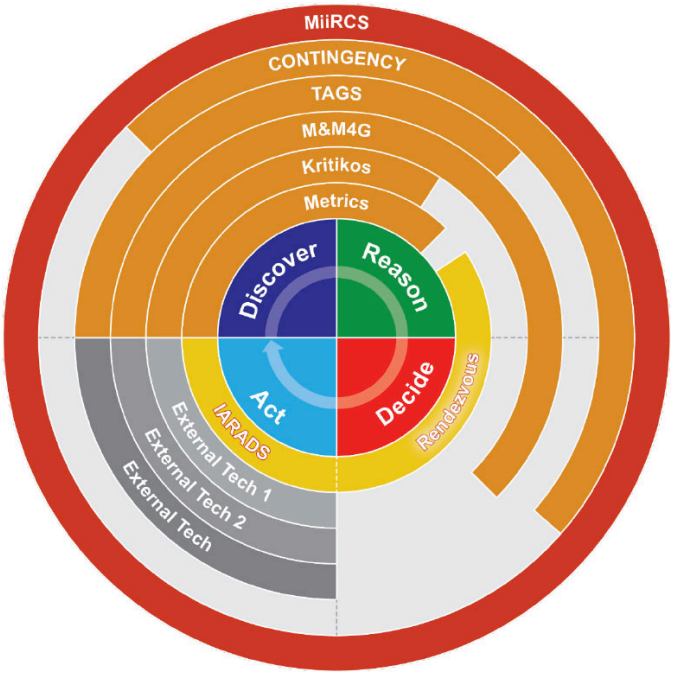
CHALLENGE

The Asymmetric Resilient Cybersecurity (ARC) initiative is placing the products of its research in a self-prescribed decision cycle to demonstrate resiliency in the face of attack. This decision cycle comprises four phases that operate in a continuous cycle: Discover, Reason, Decide, and Act. Applications distributed throughout the enterprise perform various duties within these stages in an iterative fashion to enact change in the enterprise, resulting in increased resiliency and preservation of mission critical operations. Each of these applications needs to communicate securely and efficiently in an environment with ever-changing requirements.

CURRENT PRACTICE

There are few integration solutions immediately available, of which most were developed to meet specific application requirements or missions. Other government, academia, and commercial solutions handle the integration problem using common tools and design patterns to build custom solutions. Many of these approaches leverage messaging architectures and web services to facilitate distributed communications to disparate applications throughout the enterprise. ARC has a unique and evolving set of requirements rendering existing solutions impractical for immediate progress toward resiliency demonstrations.

An integration architecture for ARC applications to achieve greater resilience in the enterprise while in a compromised state



Depiction of MiiRCS providing the integration architecture for ARC applications associated with different phases of the decision cycle.

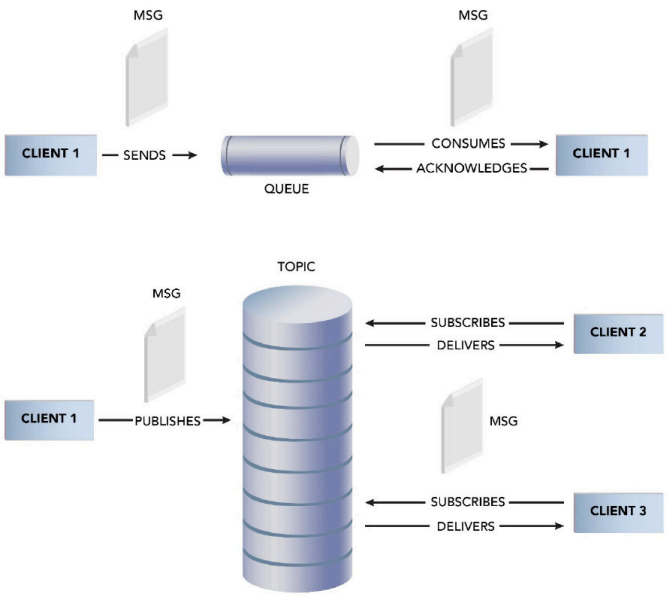
U.S. DEPARTMENT OF
ENERGY

APPROACH

The MiiRCS project focuses on two areas supporting the demonstration and measurement of a resilient enterprise. The first area is concerned with the integration of ARC research applications, and possibly other third party applications, to operate in the decision cycle. These applications perform various functions that can support resiliency and mission preservation while under attack. There are several common enterprise integration patterns from which MiiRCS has adopted an asynchronous messaging architecture using Java Enterprise Edition and the Java Message Service application programming interface. This allows any of the ARC research applications, and potentially other third party applications, to integrate in a loosely coupled and distributed fashion and overcome issues surrounding remote communications such as unreliability, latency, and availability. The second area of focus is on search and evaluation of existing tools, technologies, and applications that could be added to our integrated solution. There are many applications that have the potential to operate alongside ARC research to further increase resiliency. MiiRCS has begun documenting and ranking other research and applications from commercial, other government, and academic institutions for potential use in demonstrations.

IMPACT

The MiiRCS team will provide an integration solution, based on common tools and design patterns that can grow to meet ARC requirements as they are defined. This solution will allow for the progression



Two common messaging patterns: Point to Point using a message queue and Publish-Subscribe using a message topic.

of ARC experiments and support the development of a successful demonstration of resilient technologies. We will also continue to evaluate other tools and technologies, as they are discovered, for suitability in the ARC decision cycle, increasing the number of applications potentially leveraged to maintain mission critical functions and increase resiliency in the enterprise. In the performance of this work, a comprehension of collective communication types, used to preserve mission critical operations, will begin to evolve. With this, we hope to begin a classification or taxonomic description of such communications so that we may form a basis for development of integration architectures used to support resilient cyber infrastructures.

Contact

Jeffrey Jensen
Principal Investigator
(509) 375-3703
jeffrey.jensen@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*