# Situational Awareness Framework for Cyber Security Event Prediction and Quantification (SAFFRON)

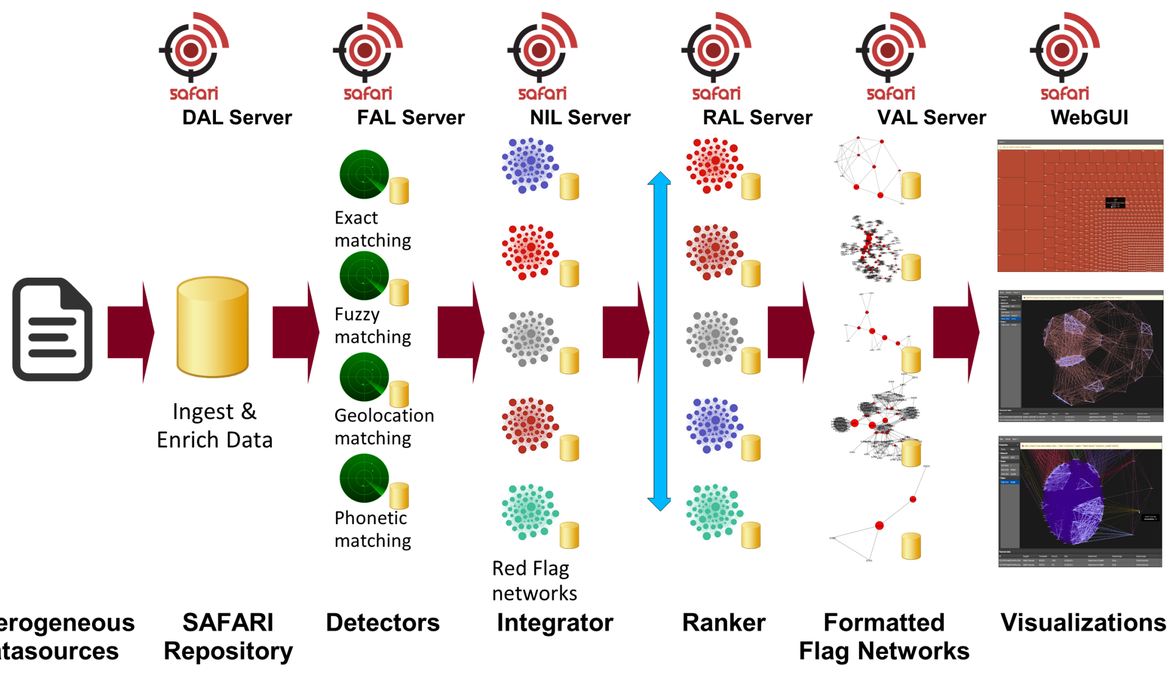
Abel Sanchez and John R. Williams

## GOALS

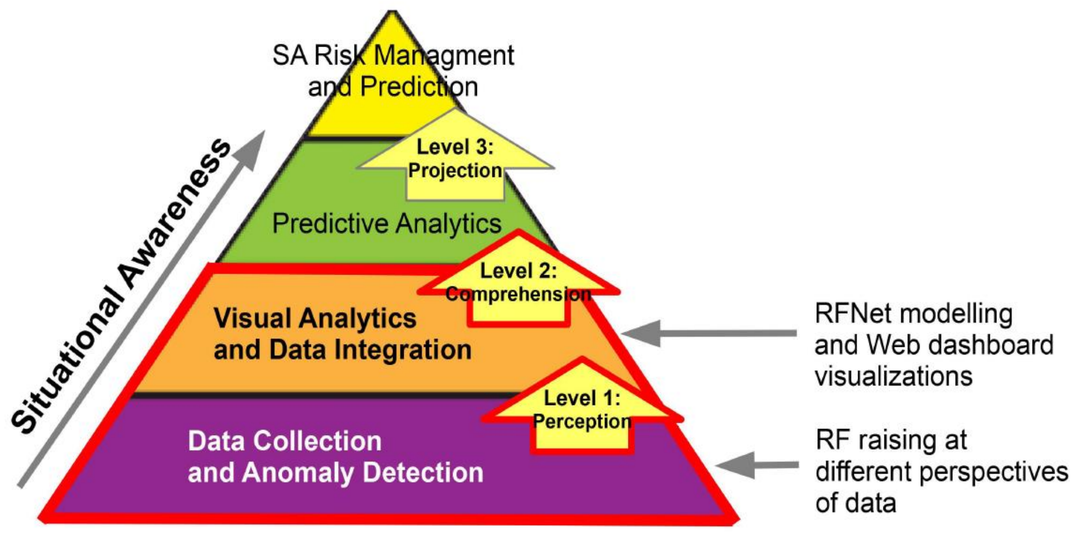
- Energy asset owners and operators do not have the capability to fully understand the risks associated with the cyber threats of today and tomorrow—risks that will continue to grow as information technology (IT) and operations technology (OT) networks increasingly merge. Without a better understanding of these risks, costs, and potential consequences, appropriate allocation of capital is a big challenge. Energy executives lack a basis for appropriate allocation of capital to the areas of greatest concern.
- The proposed research will investigate a risk modeling and data analytics platform that identifies risk tolerance and strategy for assessing, responding to, and monitoring cyber security risks on a simulation platform. The simulation will act as a proxy to the physical infrastructure.
- **Situational Awareness Framework for Cyber Security Event Prediction and Quantification (SAFFRON).** SAFFRON comprises three main components:
  - A simulator for global data infrastructures.
  - SAFARI, a risk-ranking platform.
  - STPA-Sec, a system-theoretic process analysis for security.

## RISK-RANKING PLATFORM

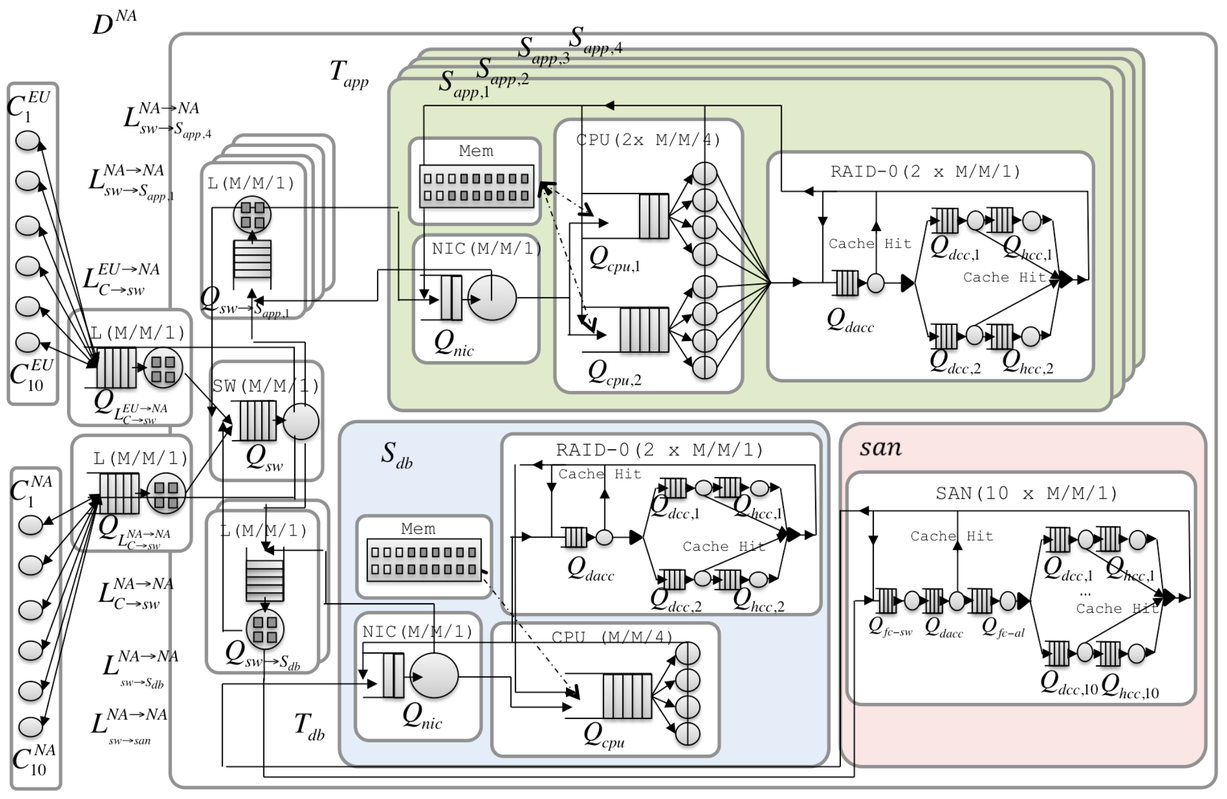
- The research team will leverage the Situational Awareness Framework for Risk Ranking (SAFARI), which they created earlier. The team will investigate a risk modeling and data analytics platform that identifies risk tolerance and strategy for assessing, responding to, and monitoring cyber security risks.
- SAFARI uses robust statistical techniques to differentiate between different types of events and their characteristics. Moreover, the research team will experiment with the use of machine learning techniques to establish control limits for event accumulation to better alert for out-of-specification cases and any systematic trends in the process, in order to take actions early on.




1. **Ingesting** rich, heterogeneous data.
2. **Enriching** data by reaching out to external data sources.
3. Running a layer of **detectors** that **match** and create linked relationships.
4. **Integrating** all linked relationships to form graphs.
5. **Ranking** risks by probabilistic analysis.
6. **Visualizing** analysis results and visualization for decision makers.




## SIMULATION PLATFORM




- The work will leverage the Large-Scale Simulator for Global Data Infrastructure created by the research team. The platform can model global infrastructures, application diversity, and background jobs, and has been validated against the global infrastructure of a Fortune 500 company.
- The information generated by the simulation platform is used for:
  - **Attack Protection**: Allows the evaluation of the effects of cyber security attacks and facilitates the design of countermeasures to fight them.
  - **Performance Estimation**: Enables the response time to be evaluated for a given workload, network topology, hardware configuration, and software application.
  - **Capacity Planning**: Enables the data center operator to determine the resources required to meet Service Level Agreements (SLA) for each distributed application running on the infrastructure.
  - **Hardware/Software Configuration**: Enables both hardware and software parameters to be calibrated to achieve optimal performance and utilization of resources.
  - **Bottleneck Detection**: Enables potential infrastructure bottlenecks to be identified and prevented.
  - **Background Job Optimization**: Facilitates the scheduling and effectiveness of jobs such as synchronization, replication, or indexing without degrading user response times.
  - **Network Administration**: Allows the topology of the global network to be designed to cope with the expected traffic while maximizing its utilization.

## SYSTEMS THEORETIC PROCESS ANALYSIS FOR SECURITY (STPA-SEC)

- The third component of the research project looks at a Systems Theoretic Process Analysis for Security (STPA). The systems approach goes beyond the technical controls and looks at organization-wide security concerns in three areas:
  - Establishes a security engineering analysis foundation.
  - Performs analysis of control actions.
  - Identifies disruption scenarios.

## FUTURE EFFORTS

- **Extend analysis & integration to other security domains.** Combine different analysis techniques for processing large amounts of unlabeled data.
- **Big data analysis.** Help subject-matter experts (SMEs) make sense of data spread across organizations by constructing more detectors. Open-source the platform to facilitate collaboration by the research community.
- **Focus.** Help SMEs focus on the most suspicious activities by extending the visual analytics libraries.



FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY