Preparing for the Future

ICS Cybersecurity and ODVA

General Session and
15th Annual Meeting of Members

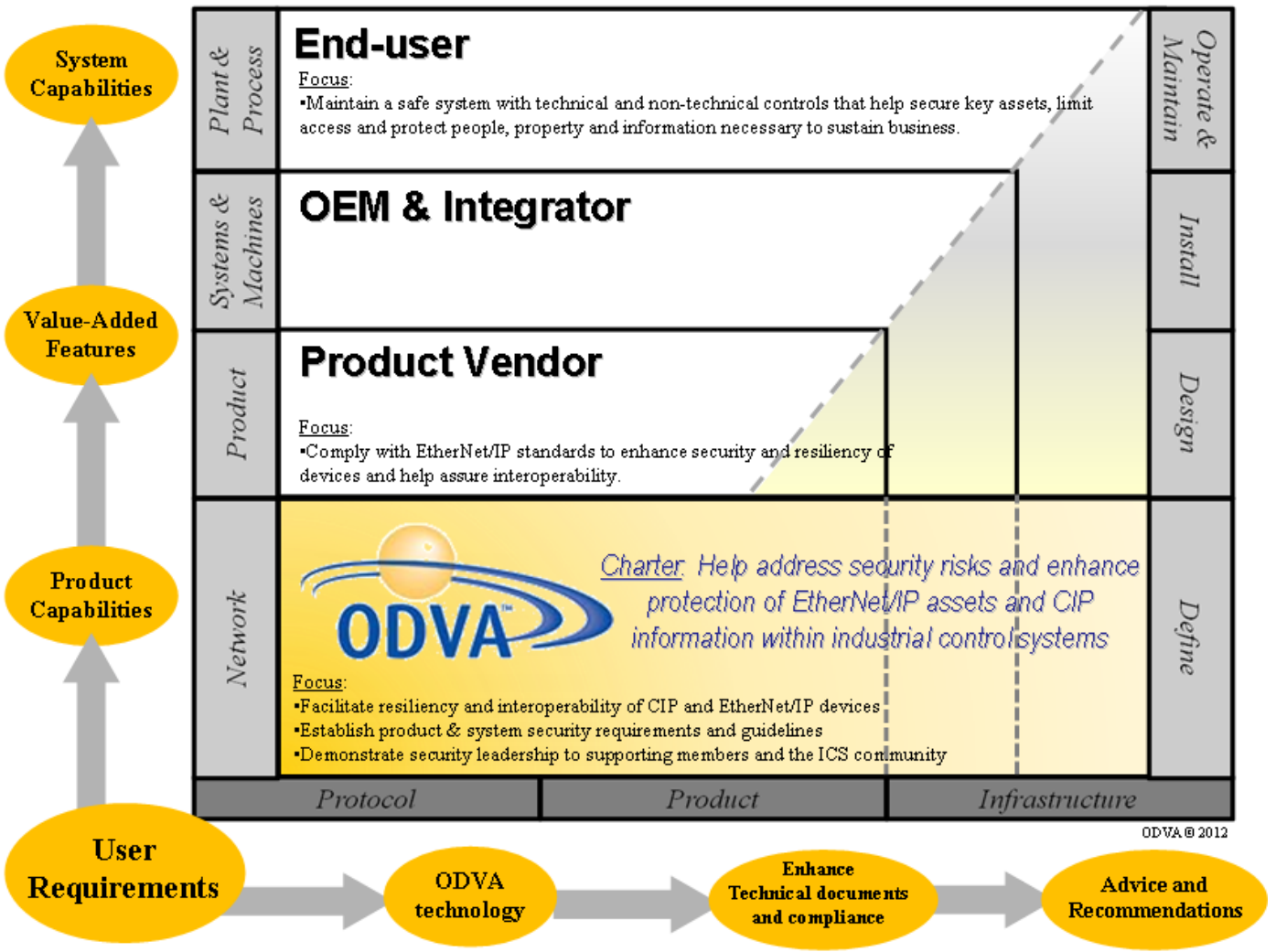
www.odva.org

Goal and Components of the Plan

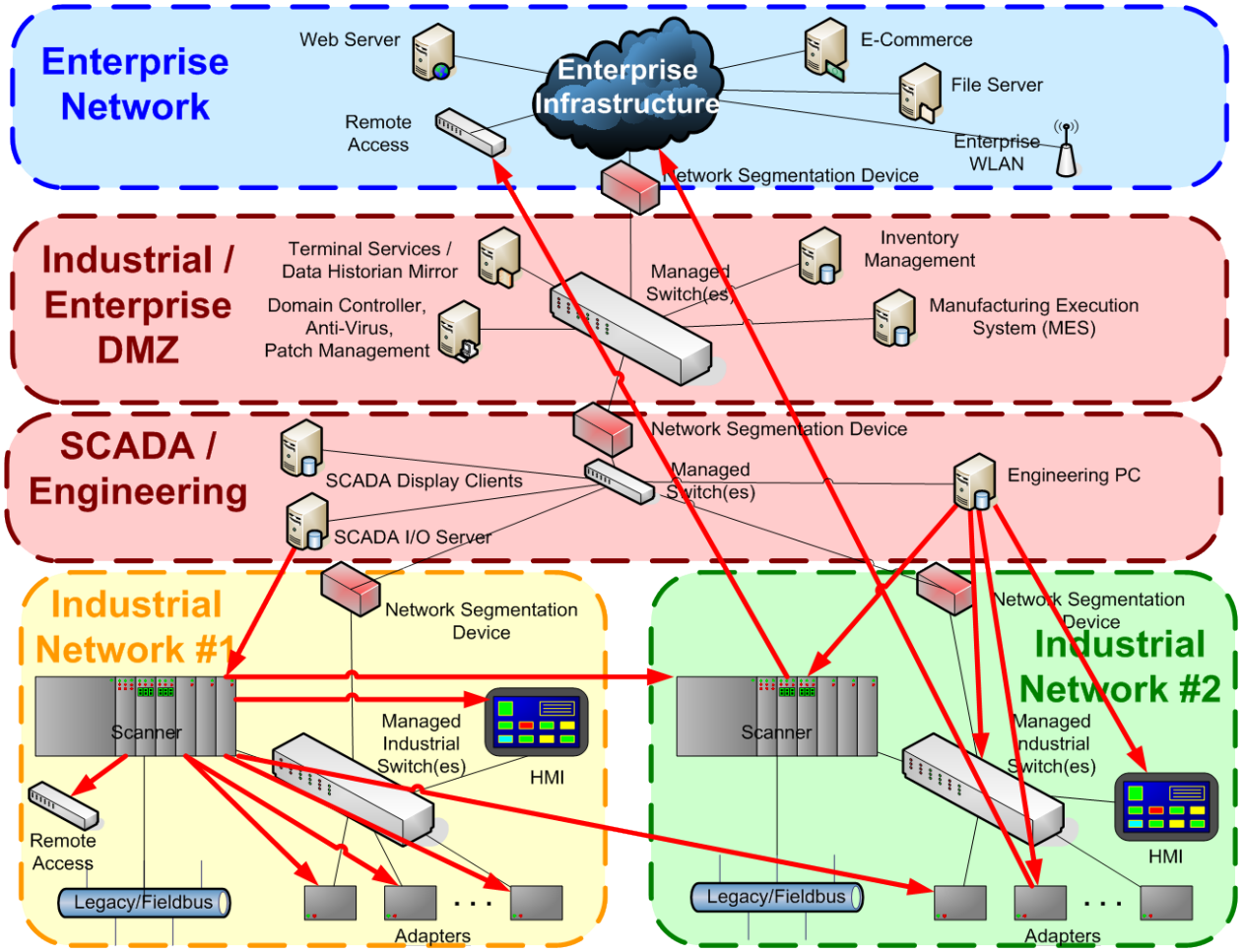
This plan defines actions within ODVA that will help manage and mitigate cybersecurity risk for adopters of ODVA technologies and EtherNet/IP and CIP in particular.

- **Major Component #1 – Establish the appropriate Role and Scope of key stakeholder groups – ODVA, ODVA vendors, and users of ODVA technology.**
- **Major Component #2 – Define the key Data Flows for which communication must be secured.**
- **Major Component #3 – Establish an ODVA Internal Business Process for Cybersecurity Risk Management and Mitigation, prescribe a recommended parallel process for ODVA vendors, and suggest a third parallel process for users.**
- **Major Component #4 – Identify the scope of Technical Work needed, who will do the work and when, plus needed alignment with 3rd party standards.**

Role and Scope of Stakeholder Groups



Key Data Flows for which Communication Must be Secured

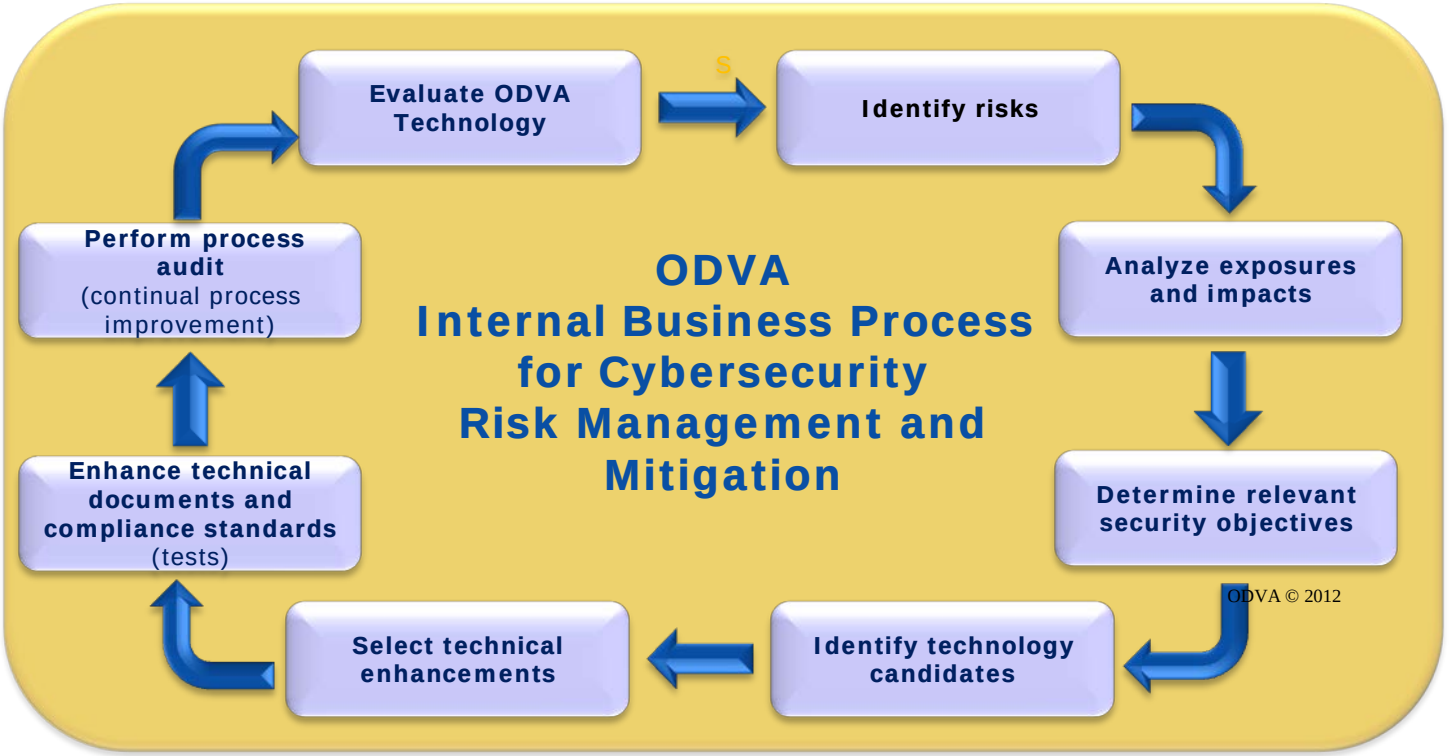


1. Scanner to Adapter process data
2. Scanner to Adapter configuration
3. Scanner to adapter across zones
4. SCADA and HMI to Adapter (PLC)
5. Scanner to Scanner
6. Engineering PC to Adapter, scanner, and HMI for configuration and diagnostics
7. Enterprise to Adapter (e.g., energy object)
8. Configuration tool to network infrastructure
9. Local Machine Remote Access
10. Enterprise remote access

Process to Manage and Mitigate Risk

Requirements Plan Will be the 1st Output of this Process

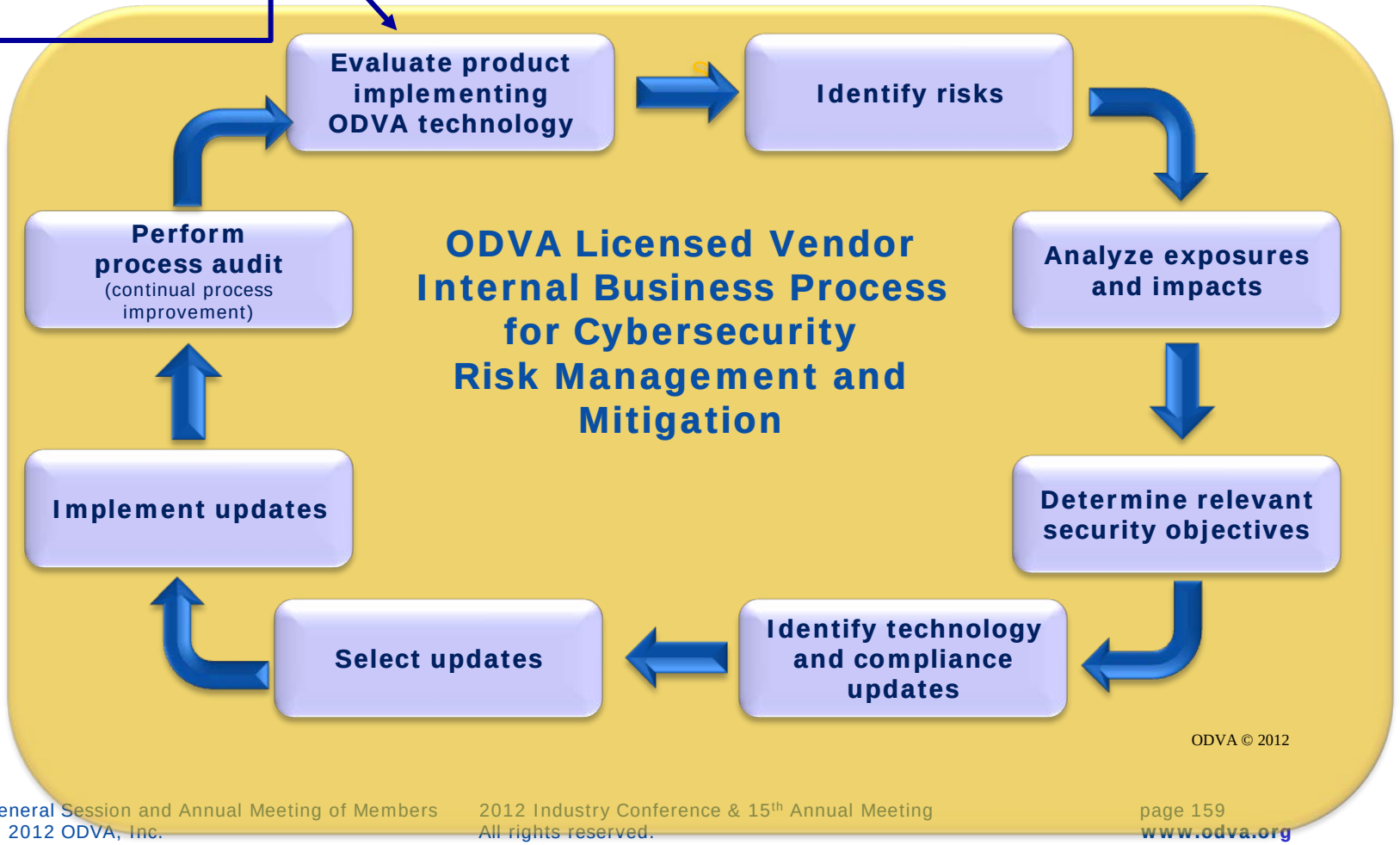
Using the ODVA internal business process for Cybersecurity Risk Management and Mitigation, the SIG for EtherNet/IP System Architecture will draft the Cybersecurity Requirements Plan. Based on the recommended scope of technical work, this plan will provide the framework for future SIG work including the proposed set of specification enhancements and their phasing.



Process to Manage and Mitigate Risk

ODVA Recommended Parallel Process for its Licensed Vendors

ODVA Technical Documents and Compliance Standards



Recommended Scope of Technical Work

1) Harden all EtherNet/IP™ end-points

- Define base-level product hardening requirements
- Rationalize CIP™ services defaults and conditional use
- Conformance test coverage expands, in-line with industry standards, to include product resiliency

2) Protect CIP™

- Define and allow CIP communication through secure tunnels
- Focus on technology, interoperability, and usability
- Document recommended use
- Conformance test coverage expands to evaluate interoperability of EtherNet/IP devices using secure tunnels

3) Secure CIP™

- Requirements Plan
- Define media independent, end-to-end security in CIP
- Conformance test coverage expands to evaluate secure protocol (i.e., CIP)

Recommended Alignment of Technical Work with 3rd Party Standards

Why align with Selected 3rd Party Standards?

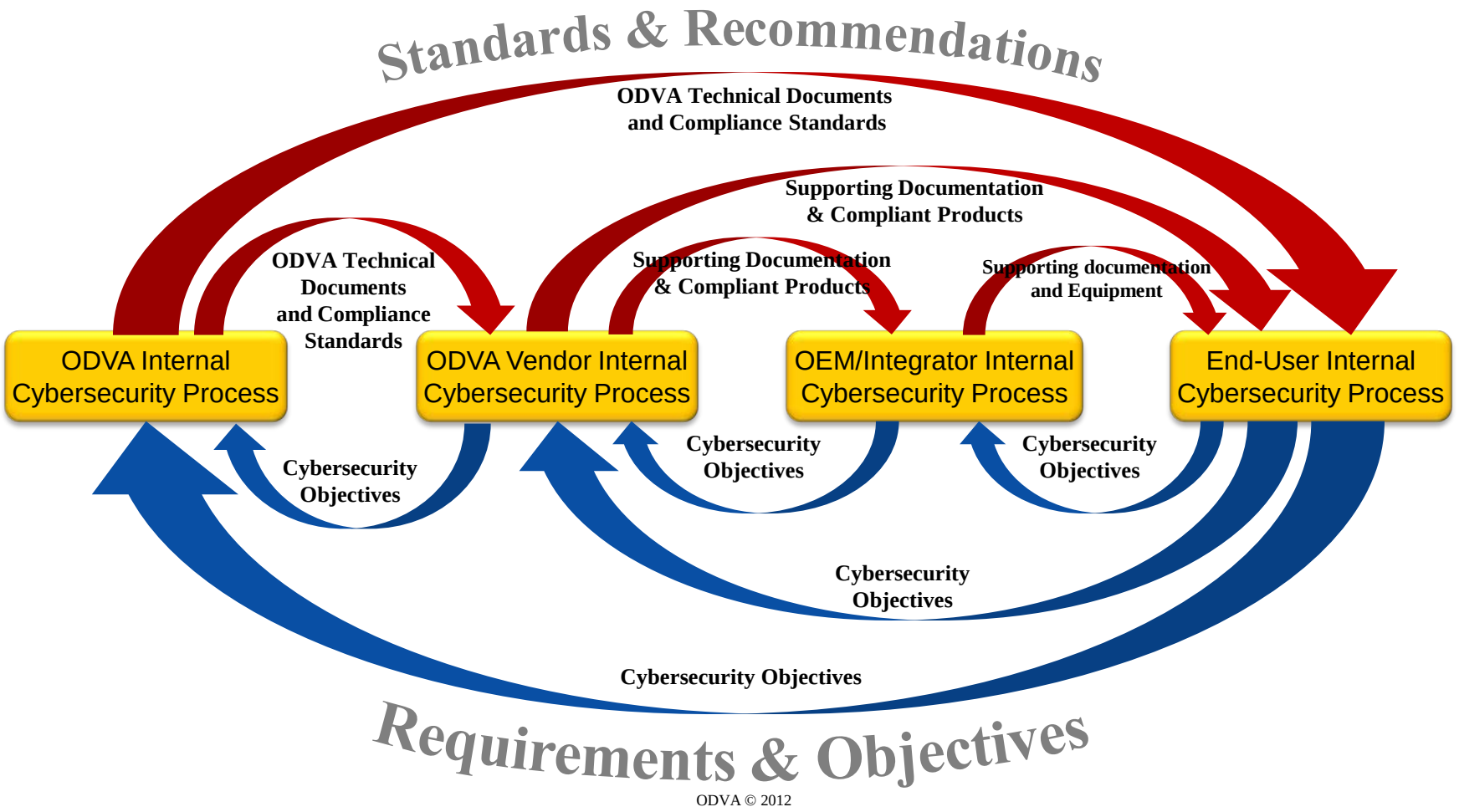
- Strengthens ODVA's position within the ecosystem through awareness versus isolation.
- Simplify ODVA, Vendors and End-users investments by providing a single set of recommendations and certification where appropriate.
- Focus ODVA influence in areas where value can be added (EtherNet/IP and CIP).

Identified Influential Standards		
IEC TC65 / IEC62443	Devices, Systems, OEM/SI, End-users	Prevalent standard in the future
ISA99	Devices, Systems, OEM/SI, End-users	Content will be submitted to IEC62443
ISCI / ISA Secure	Device and System certification	Expected to become IEC certification

Recommendations

- Align ODVA recommendations with IEC 62443 recommendations for systems, OEM/SI and End-users.
- Adopt IEC 62443 recommendations for device robustness during conformance testing.
- Offer the market a path to go beyond IEC standards with specific recommendations and certification for EtherNet/IP and CIP.
- Demonstrate alignment with IEC through documented ODVA participation and influence if possible (i.e., Liaison D status or similar structure)

External Process Interactions Cybersecurity Risk Management and Mitigation



Supplemental Information on the Task Force

Current Participants

- **Volker Alt**
  Project Director, Ethernet-based Fieldbus – Bosch Rexroth
- **David Doggett**
  Program Director, Industry Cyber Security – Schneider Electric
- **Rich Harwell**
  Chief Technology Officer – ODVA
- **Ludwig Leurs**
  Project Director Ethernet Convergence – Bosch Rexroth
- **Adrienne Meyer**
  Manager, Membership and Marketing Communications – ODVA
- **Brian Uffelman**
  Senior Manager, Product Management for Software & Security – Cisco Systems
- **Katherine Voss**
  Executive Director – ODVA
- **Doug Wylie**
  Manager, Industrial Security Program - Rockwell Automation