

# **Antivirus for Industrial Control Systems**

**Moderator: David Teumim, CISSP  
Independent Consultant, Teumim Technical, LLC**

# Use of Antivirus Software on Industrial Control Systems

## A DOE National SCADA Test Bed Project

**Joe Falco**, National Institute of Standards and Technology (NIST)

**Steve Hurd**, Sandia National Laboratories (SNL)

**Dave Teumim**, Teumim Technical, LLC (Consultant for SNL)



## Project Summary

- ◆ **Document a set of guidelines and a test methodology for industry to use when implementing antivirus software on industrial control and SCADA systems**
- ◆ **Collaborative effort between NIST and the DOE National SCADA Test Bed at Sandia National Laboratories**

Note: Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

# Industry Participants

## ◆ Participants Include

- End Users
- Control Vendors
- Antivirus Vendors
- Government Labs

## ◆ Current practices and other feedback

## ◆ Document Review

## ◆ Pilot Testing

# Why This Project?

- ◆ **This project was created in response to feedback from industry**
- ◆ **Control system engineers expressed concerns of running antivirus software on their control systems**

## Antivirus Attitudes in 2003

- ◆ Antivirus will “break” control systems
- ◆ Control vendors won't support it
- ◆ Antivirus will use critical computing capacity and resources when needed for process control
- ◆ Antivirus updates and maintenance too much trouble/time consuming

# What We're Finding in the 2005/2006 Timeframe

## Control Suppliers

### Degree of Vendor Support Varies:

- “Embedded”
- Certified with use instructions
- Good to use but not certified
- Use at your own risk

# End User Spectrum

## End Users Fall into Three General Categories

- Early Adopters (Tend to retrofit)
- Phase-in gradually (with new equipment)
- Don't install on any systems

# Test Methodology

- ◆ **Establishing a performance baseline – the level of performance you can reliably expect during system usage and workload**
- ◆ **Generic Performance Test Procedures**
  - Based on different operational modes of antivirus

# Project Deliverables

## Provide industry with a report that includes:

- Implementation guidance and “Good Practices” (culled from plant visits, industry interaction, and vendor feedback)
- Step-by-step test procedures (to determine the impact antivirus software will have on a control system’s performance) and pilot data
- Information from plant visits (how companies are currently addressing the issues)

## Introducing the Panel

- ◆ **Jae Pudewell**                      **McAfee, Inc.**
- ◆ **Bryan Kingsford**                **Symantec Corp.**
- ◆ **Mark Heard**                        **Eastman Chemical Co.**
- ◆ **Ernie Rakaczky**                  **Invensys Foxboro**
- ◆ **Richard Clark**                    **Invensys Wonderware**

# Antivirus Panel

- ◆ Jae D. Pudewell, Sr. Product Manager, McAfee, Inc.
  - VirusScan Enterprise and AntiSpyware Enterprise
- ◆ **Involvement with Antivirus:**
  - Direct AV involvement for about two years as VSE product manager
  - Over eight years experience with IT security products
- ◆ **Antivirus Position:**
  - Malware is not Process Industry unique, though do have some inviting targets
  - As Process Industry increasingly adopts industry-standard infrastructure, it will see the same benefits and risks
  - Key is for Process Industry to retain control, but adapt and adopt IT tools and technology to unique environments
    - May also require process change and evolution

# Antivirus Panel

- ◆ Bryan Kingsford, CISA, CISSP, Chief Architect, Office of the CTO, Symantec Corporation
- ◆ **Involvement with Antivirus:**
  - Technology specialist applying information security solutions in industrial control environments
- ◆ **Antivirus Position:**
  - Work with industrial control vendors to insure performance levels are not impacted
  - Properly address software and security content update issues unique in this environment
  - Provide multi-layer security solutions to maximize coverage while minimizing impact
  - Participate in efforts related to this area such as this antivirus study and this PCSF Meeting

# Antivirus Panel

- ◆ Mark Heard, Engineering Associate, Eastman Chemical Company
- ◆ **Involvement with Antivirus:**
  - Testing AV SW (and updates) on development systems in Control Systems Lab
- ◆ **Antivirus Position:**
  - Company policy requires networked nodes to have current AV SW where possible
  - Concerned, but haven't observed any problems with AV SW first-hand
  - Would like not to use AV SW

# Antivirus Panel

- Ernest A. Rakaczky – Program Manager of Control System Security at Invensys/Foxboro
- **Involvement with Antivirus:**
  - Currently have embedded McAfee Antivirus in all XP stations & 2003 Servers shipped from the factory – since April 2005. Clear guidelines on implementation for legacy installed systems.
  - Active participation & Support of current study
- **Antivirus Position:**
  - Value is in the ability to keep current
  - Difficult to keep signatures current within a Control System
  - The need to keep the Anti-Virus protection layer as distinct as possible
  - The need to create safe updating tools and processes

# Antivirus Panel

- ◆ Rich Clark, INFOSEC Analyst, Invensys Wonderware
- ◆ **Involvement with Antivirus:**
  - Provide guidance for AV use to end customers
  - Working with Industry Standards Organizations
- ◆ **Antivirus Position:**
  - Does not recommend using AV or 3<sup>rd</sup> party software on control system machines
  - Recommend isolating Control and SCADA Systems using IPSec and secure routing
  - Recommend installing AntiVirus hardware/software only on Gateway devices.

# Antivirus Workshop Agenda

- ◆ Continue panel
- ◆ Audience Q&A
- ◆ Start a PCSF Antivirus Interest Group ?