Setting the Standard for Automation™

Guidance and Performance Impact Testing to Support the use of Antivirus Software on SCADA and Industrial Control Systems

EXPO 2005

Chicago, IL

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Presenter

- Joe Falco is a mechanical engineer in the Intelligent Systems Division of NIST's Manufacturing Engineering Laboratory. One of his primary responsibilities within the NIST Homeland and Industrial Controls Security Program is the development and implementation of the NIST Industrial Control Security Testbed. Current testbed activities are focused on the development of guidance, performance metrics and tests that industry can use to mitigate potential problems encountered during the deployment of security software and hardware in industrial control systems. His presentation today discusses one of these efforts in the deployment of antivirus tools.

Project Summary

- Produce a set of guidelines and a test methodology for industry to use when implementing antivirus software on Industrial Control and SCADA systems
- Guidelines and test methodology are based on a survey of current industry practices and laboratory testing
- Collaborative effort between the National Institute of Standards and Technology (NIST), and the Department of Energy's 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.

Guidelines and Test Methodology

- For industry use when deploying antivirus software on workstations and servers that are running control system applications (HMI, control server, data historian, software PLC)
  - **Guidelines** – based on an industry survey of end-users and vendors who are currently deploying antivirus software on their systems as well as on testbed experience
  - **Test Methodology** – a set of general test procedures focusing on performance impacts to be used as a starting point when developing control system specific test procedures
  - **Test Cases** – laboratory based example test implementations using the test methodology with an analysis of test results

Audience

- End users who have never implemented antivirus on their systems for fear that it may disrupt their production
- End users implementing a different antivirus application than that specified and certified by the control system vendor
- End users concerned with the effects that antivirus software may have on the performance of their control system
- Control system vendors implementing, specifying, or certifying the use of antivirus software on their systems

Guidance

- Primarily based on results of an industry survey of end-users and vendors currently using or recommending the use of antivirus software with their control systems
- Integration Guidance such as:
  - Antivirus configuration settings and possible effects on performance
  - Advice on scheduling manual scanning operations and virus definition updates
- **Disclaimer:** Any vendor guidance specific to control system and antivirus software compatibility should be given precedence over this generic guidance.

Test Methodology

- Compatibility and Functionality Testing
- Identification of processes and performance variables to monitor
- Establishing a performance baseline – the level of performance you can reliably expect during system usage and workload
- Generic Performance Test Procedures
  - Manual (On-Demand) Scanning
  - Active (On-Access) Scanning
  - Virus Definition Update

Test Cases

- Laboratory based example test implementations using the test methodology with an analysis of test results
- Current test cases were developed in government laboratories
  - Test Case 1: NIST Industrial Control Security Testbed – HMI
  - Test Case 2: PNNL SCADA Testbed – HMI
- Additional test cases from industry and government laboratories will be included as they become available

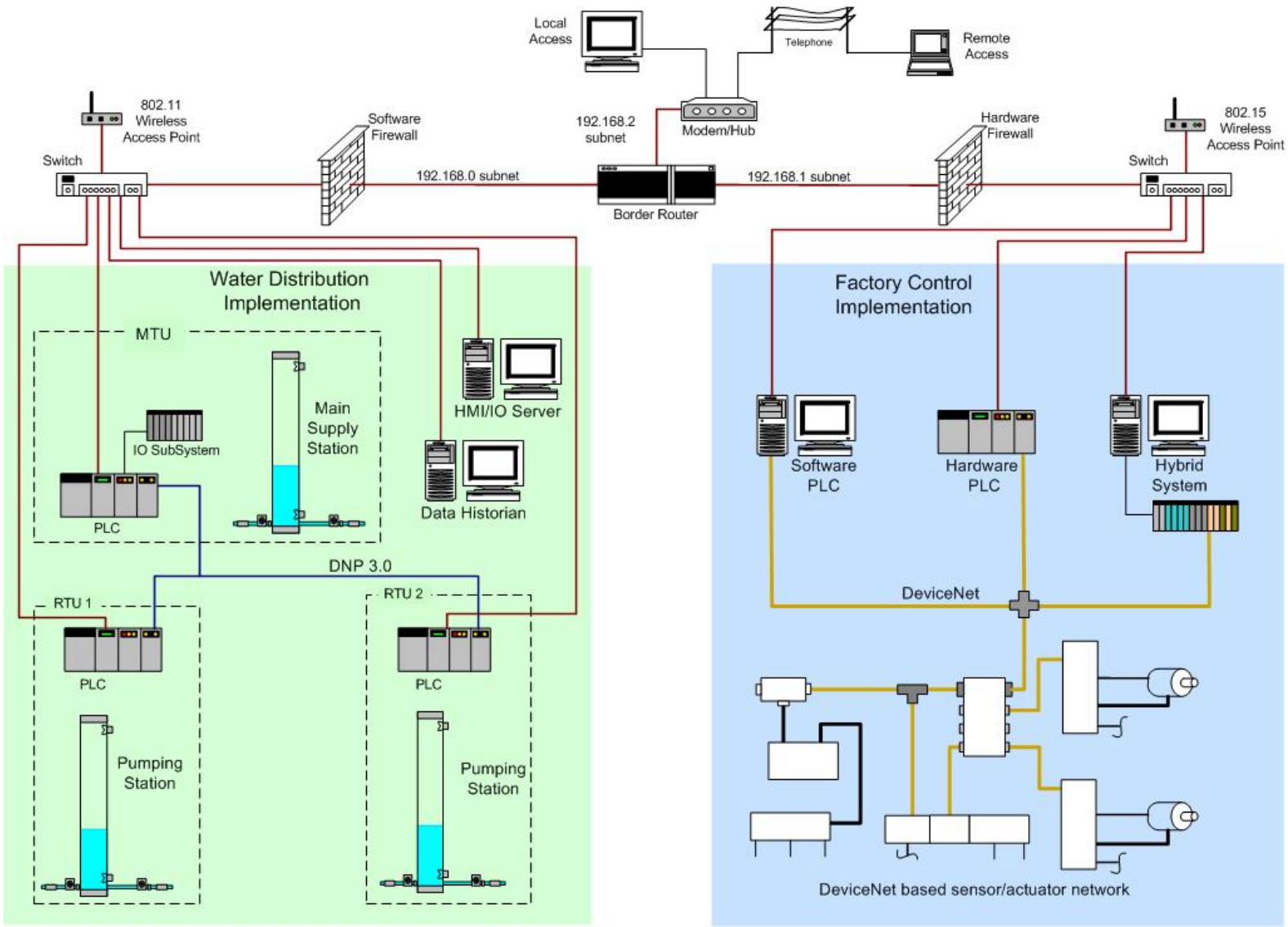
Test Case 1 Overview

- Generated using the NIST Industrial Control Security Testbed
- Industrial control based HMI and I/O Server running on a Windows 2000 PC Platform with a concurrently running antivirus software application
- Compare baseline operation of HMI software with its operation concurrent to 3 modes of operation of an antivirus software package

Test Case 1
NIST Industrial Control Security Testbed

- **Disclaimer:** Commercial equipment and materials are identified in order to adequately specify certain systems. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, Sandia National Laboratories, or the Department of Energy, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.
- **Disclaimer:** Products undergo testing to determine the validity of the testing procedures and the range of results that can be expected with commercial systems. Any results will be reported either in aggregate, or with any vendor-identifying information removed.

NIST Industrial Control Security Testbed : Architecture

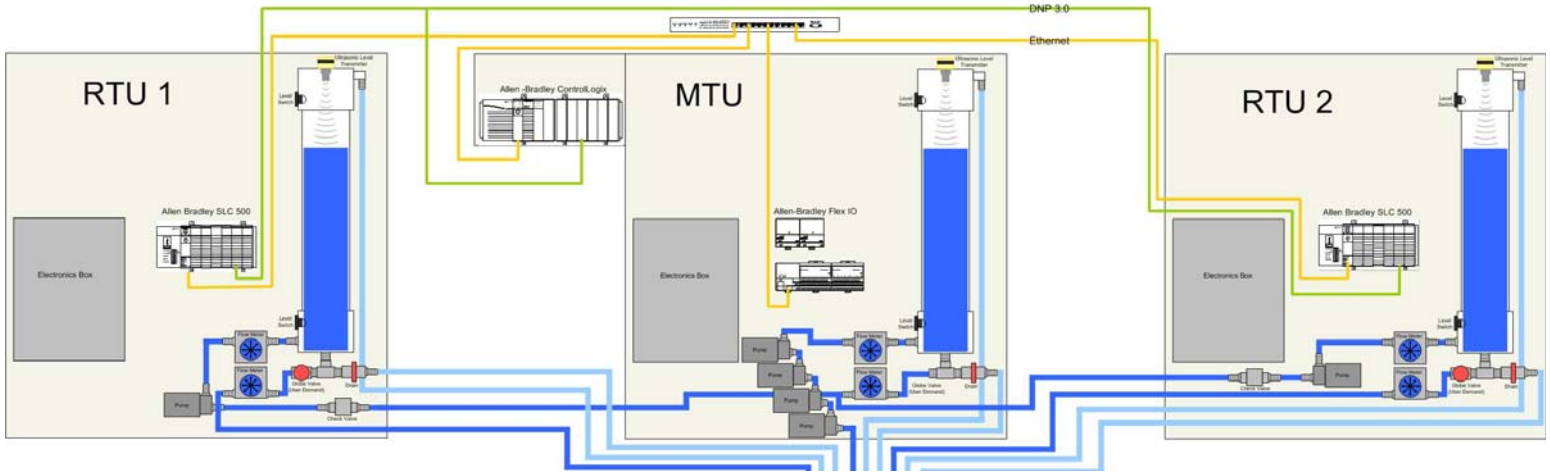


Factory Control Implementation

- DeviceNet I/O network
- Three controller options
  - Software PLC
  - Hardware PLC
  - Hybrid Controller
- Historian
- HMIs

Water Distribution Implementation: Layout

- Hardware PLCs
- Ethernet & DNP3.0
- Historian and HMI

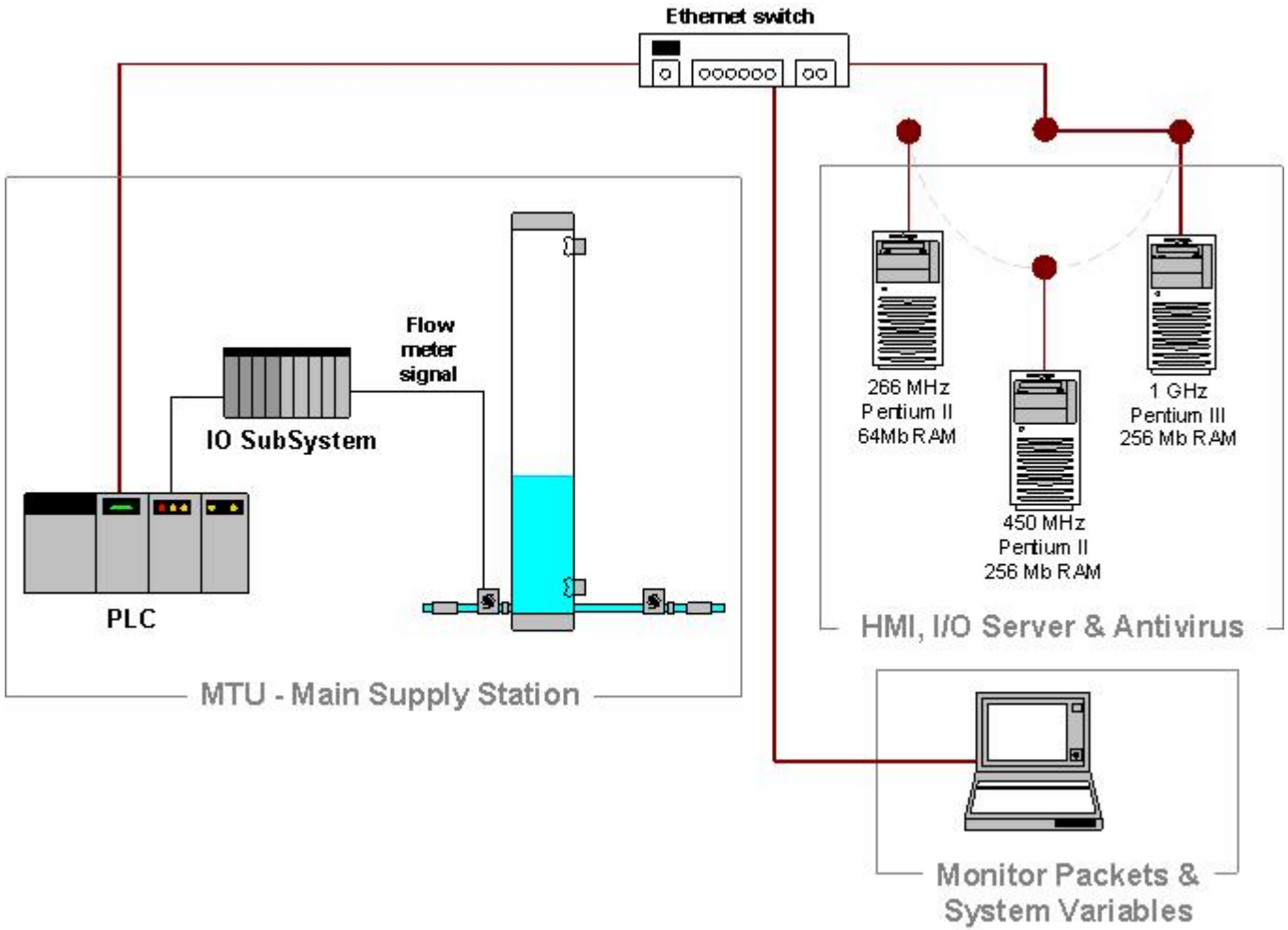


Water Distribution Implementation: Lab Photo

Test Case 1: Experimental Setup

- 3 PC platforms that address typical lower end PCs considered the most vulnerable to performance impacts caused by the inclusion of antivirus software
- HMI application and PLC programmed to bring baseline operation of each PC to a 40-60% total CPU utilization
- Use of the EICAR test virus to analyze virus detection and removal affects
- Performed experiments with antivirus Manual and Active scanning as well as Virus Definition Update operations
- Collected total and individual process CPU utilization data
- Recorded polling latency for a single sensor signal
- Compared data between control system baseline operation to control system operation with concurrently running antivirus operations

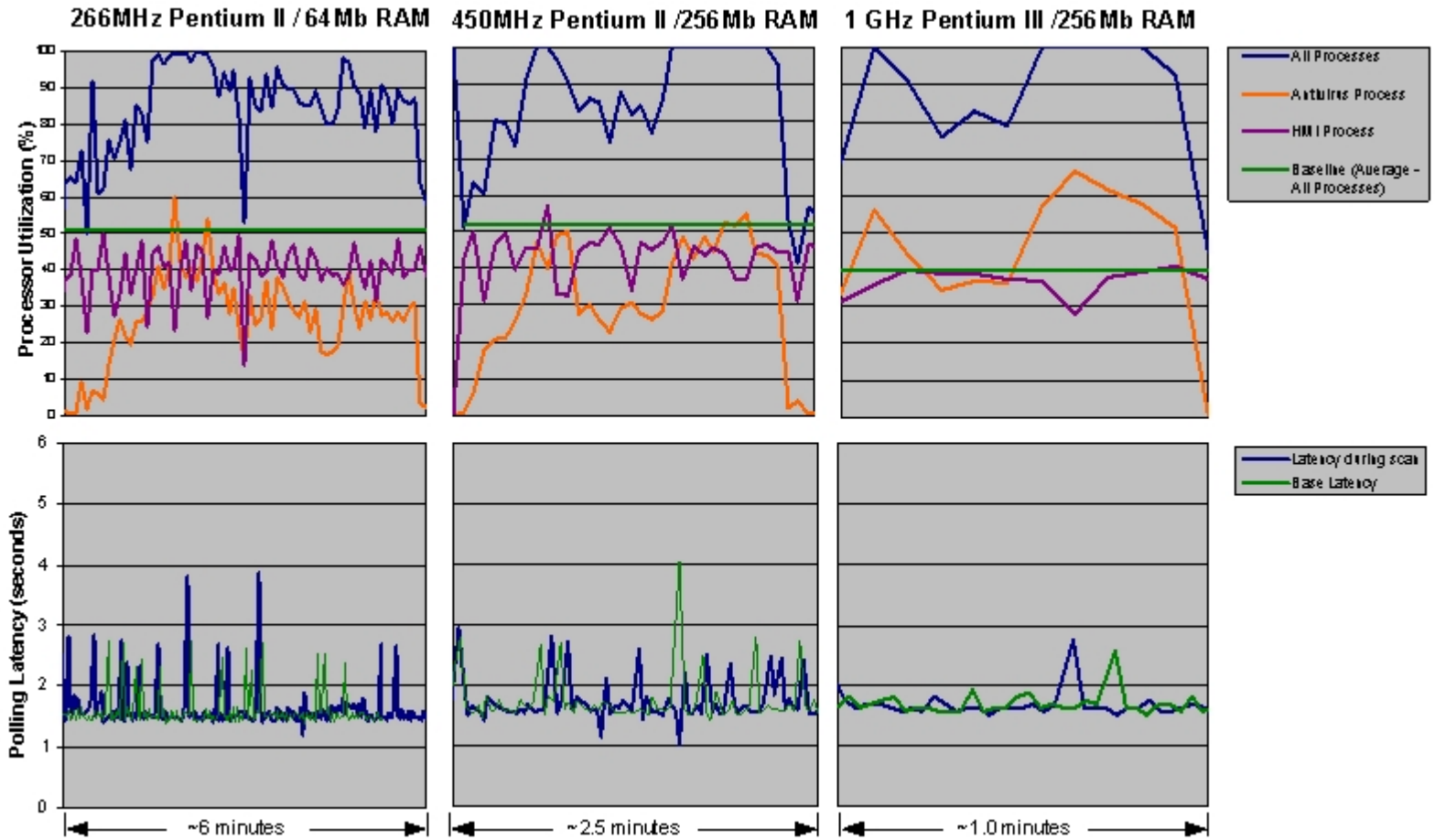
Test Case 1: Experimental Setup



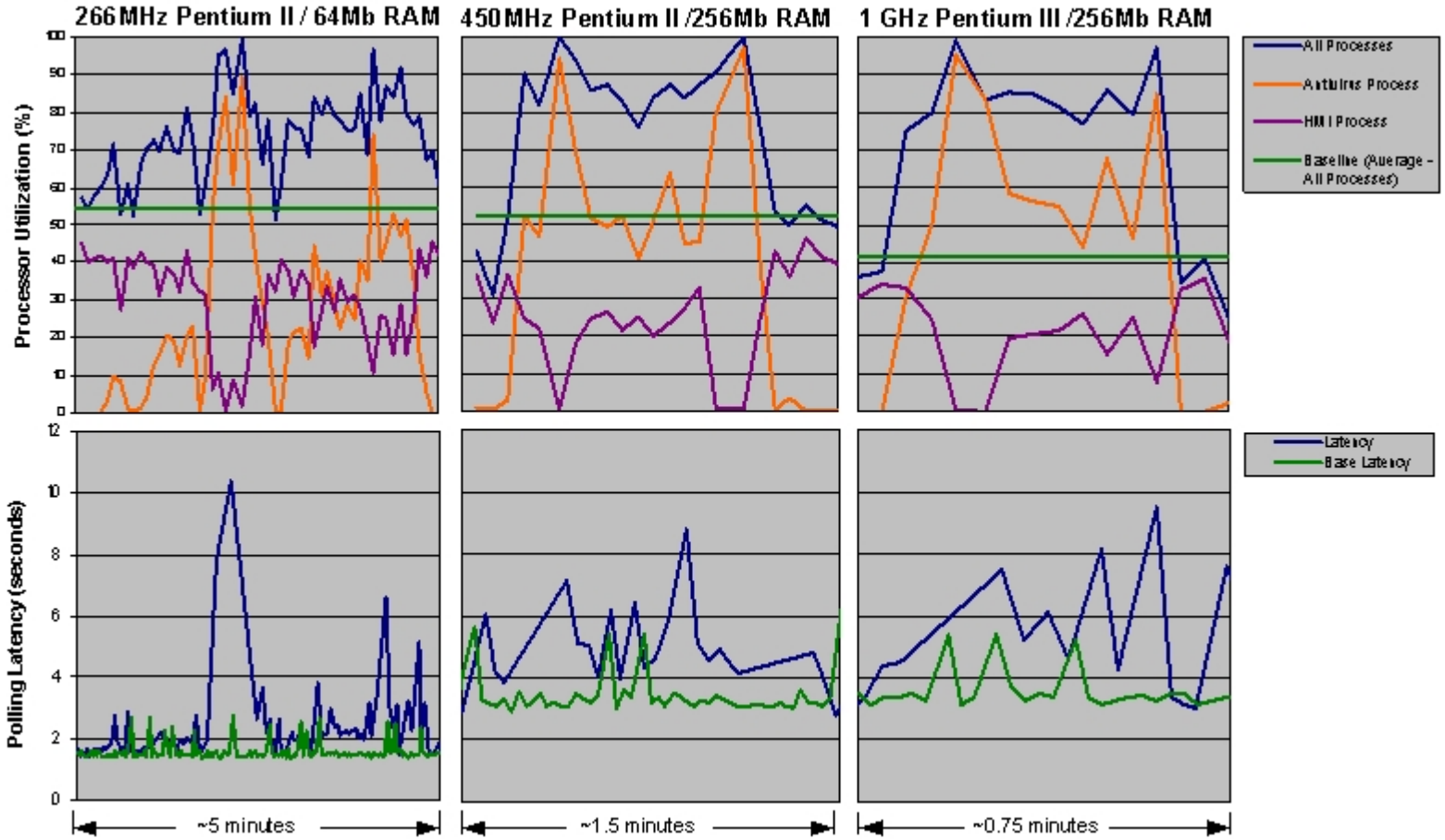
Test Case 1:
Manual (On-Demand) Scanning

- Manual scanning performed on 100MB folder containing 1000 small file including multiple copies of EICAR virus
- Detection and removal of the EICAR virus instances had no significant effects on performance
- Testing performed over different throttling settings – the amount of CPU time dedicated to the antivirus application
- Total CPU utilization reached 80% to 100% regardless of the throttling setting
- When throttling set to maximum, antivirus process dominated CPU time causing a loss in HMI process CPU time.
- When set to the lowest throttling setting, the antivirus process only used remaining CPU time
- The highest throttling setting produced more chaotic latency patterns with larger latency spikes than the lowest setting

Test Case 1:
Manual (On-Demand) Scanning- Low Priority



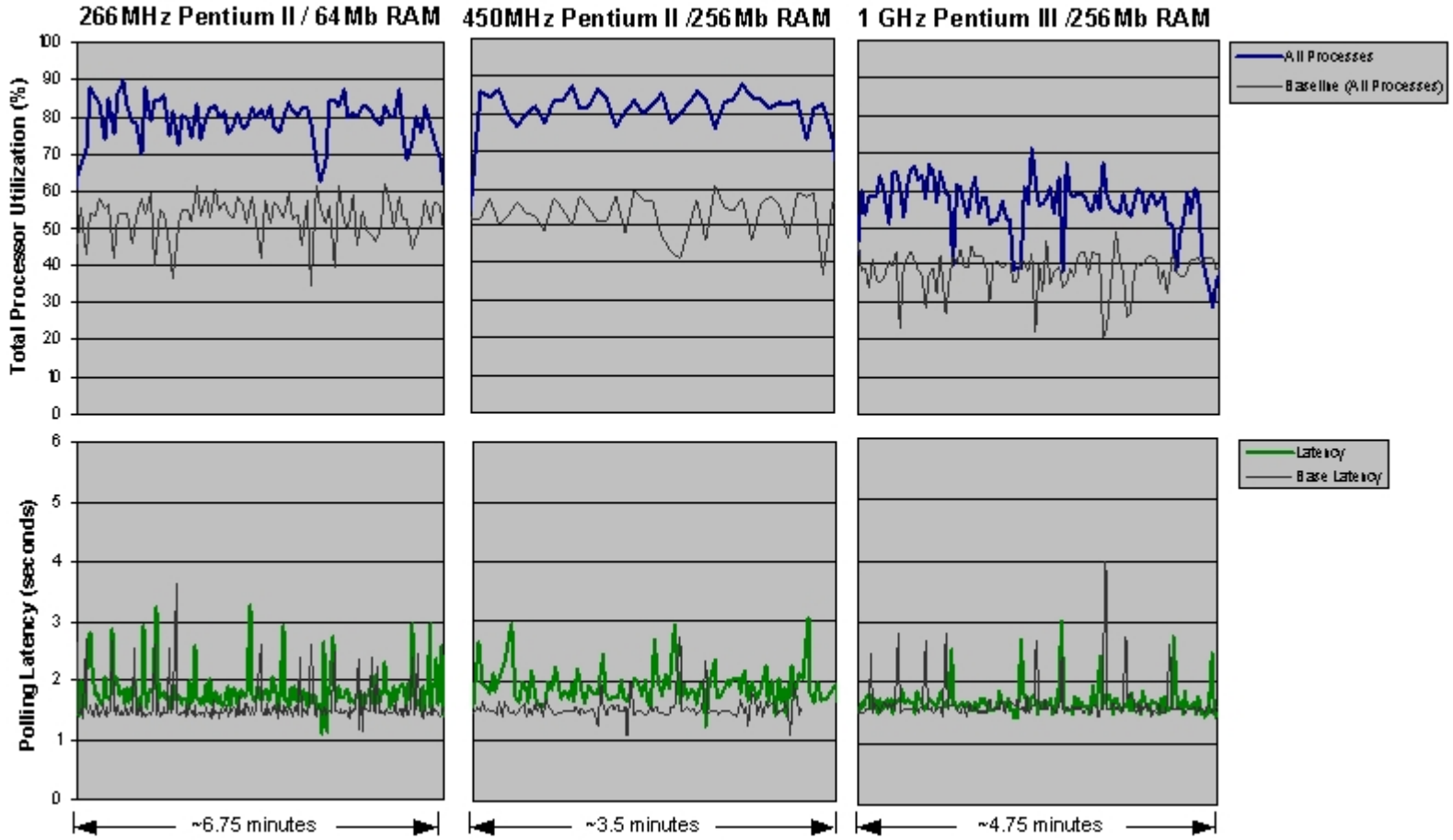
Test Case 1:
Manual (On-Demand) Scanning- High Priority



Test Case 1:
Active (On-Access) Scanning

- Same 100 MB directory transferred from a removable hard drive to the test system hard drive
- Detection of the EICAR virus had no significant effects on performance
- Active scanning had minimal impact on HMI performance from comparison of baseline and scanning latency measures as well as individual process CPU utilizations
- Analysis of individual process utilizations indicates that the increase in total processor utilization was primarily due to the file transferring process

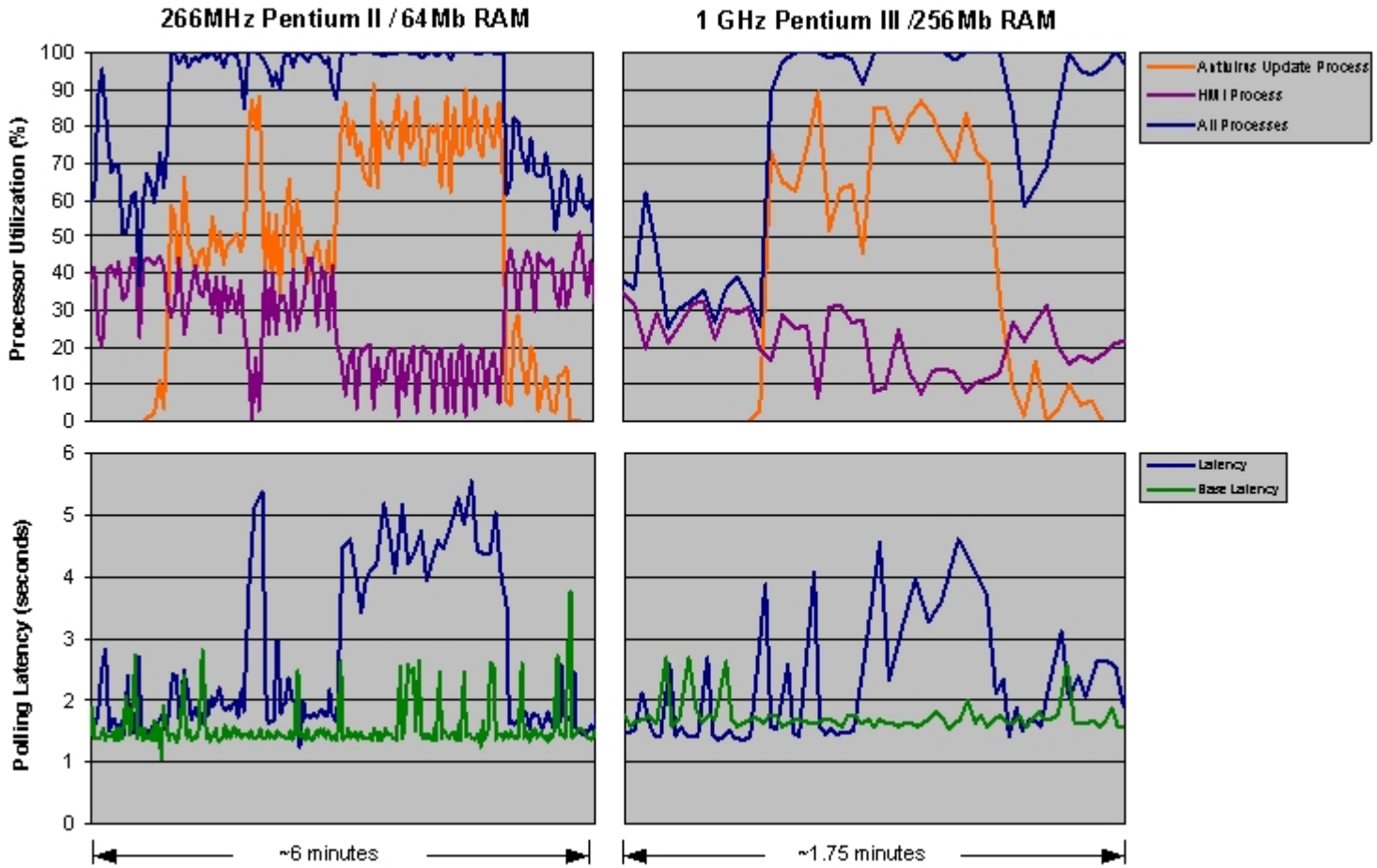
Test Case 1:
Active (On-Access) Scanning



Test Case 1:
Virus Definition Update

- Performed a virus definition update using a local update file that was downloaded from an antivirus vendor site
- Monitored performance variables throughout the update process
- Update utility dominated processor utilization
- 100 % CPU utilization throughout update on all three platforms
- Noticeable performance loss on HMI processes as well as others
- Significant polling latencies were observed throughout the update process

Test Case 1:
Virus Definition Update



Guideline and Methodology Document Status

- First draft reviewed by industry and government participants
- Second draft is now complete. We need industry feedback and pilot testing
- Expanded test case1 to include larger loads on the HMI application and are currently generating data for a second antivirus software brand
- Test case 2 is being documented as a result of pilot testing conducted at Pacific Northwest National Laboratory (PNL)
- Considering additional test cases:
  - Data Historian
  - PC Based PLC
  - SCADA Server

Acknowledgements

- Co-Authors: Michael Lochner, Dave Teumim
- End user and vendor participation
- PNL pilot testing/test case 2
- Sandia National Laboratories

Questions ?