GE Power

POWER SERVICES ENGINEERING
PRODUCT SERVICE

TIL 1881-R2
21 JANUARY 2016
Compliance Category – M
Timing Code - 6

TECHNICAL INFORMATION LETTER

NETWORK SECURITY TIL FOR MARK™ V, VI AND VIE CONTROLLER PLATFORMS

APPLICATION

All control panels using Mark V or Mark Ve and Mark VI or Mark VIe control platforms. Includes the following Mark VI, VIe, Mark V, Ve generation controllers: EX2100, EX2100e, LS2100, LS2100e, and Mark VIeS systems. All "Windows" based HMI systems that are setup with remote access are included. The legacy <I> DOS systems are not included.

PURPOSE

To advise sites of new recommendations to help improve control system robustness to potential cyber-attack.

REASON FOR REVISION

To update the reference documentation to reflect migration of GHT-200042 to GEH-6808.

Compliance Category

M - Maintenance	Identifies maintenance guidelines or best practices for reliable equipment operation.
C - Compliance Required	Identifies the need for action to correct a condition that, if left uncorrected, may result in reduced equipment reliability or efficiency. Compliance may be required within a specific operating time.
A - Alert	Failure to comply with the TIL could result in equipment damage or facility damage. Compliance is mandated within a specific operating time.
S – Safety	Failure to comply with this TIL could result in personal injury. Compliance is mandated within a specific operating time.

Timing Code

1	Prior to Unit Startup / Prior to Continued Operation (forced outage condition)
2	At First Opportunity (next shutdown)
3	Prior to Operation of Affected System
4	At First Exposure of Component
5	At Scheduled Component Part Repair or Replacement
6	Next Scheduled Outage

BACKGROUND DISCUSSION

When the Mark VI and VIe control systems were developed, these controllers were envisioned to work on isolated private networks with no connectivity outside the plant. Over time, the need to take advantage of remote maintenance and diagnostic services has resulted in increased levels of interconnectivity with corporate networks. This has created a potential exposure risk of cyber-attack.

There are generally 3 separate networks found in Mark VI and Mark VIe controller platforms

UDH – Unit Data Highway – Transports data and commands between the controller panels and the HMI / OSM (On-site monitor)

PDH – Plant data highway – Transport data between HMIs and the DCS (distributed control system) and /or OSM and / or RSG. Not connected to control panels.

IONET – transports data between the controller and IO circuit boards. On Mark VI platforms this is a small Thinet (COAX) based network but on Mark VIe this network forms the extensive internal "backplane" of the controller.

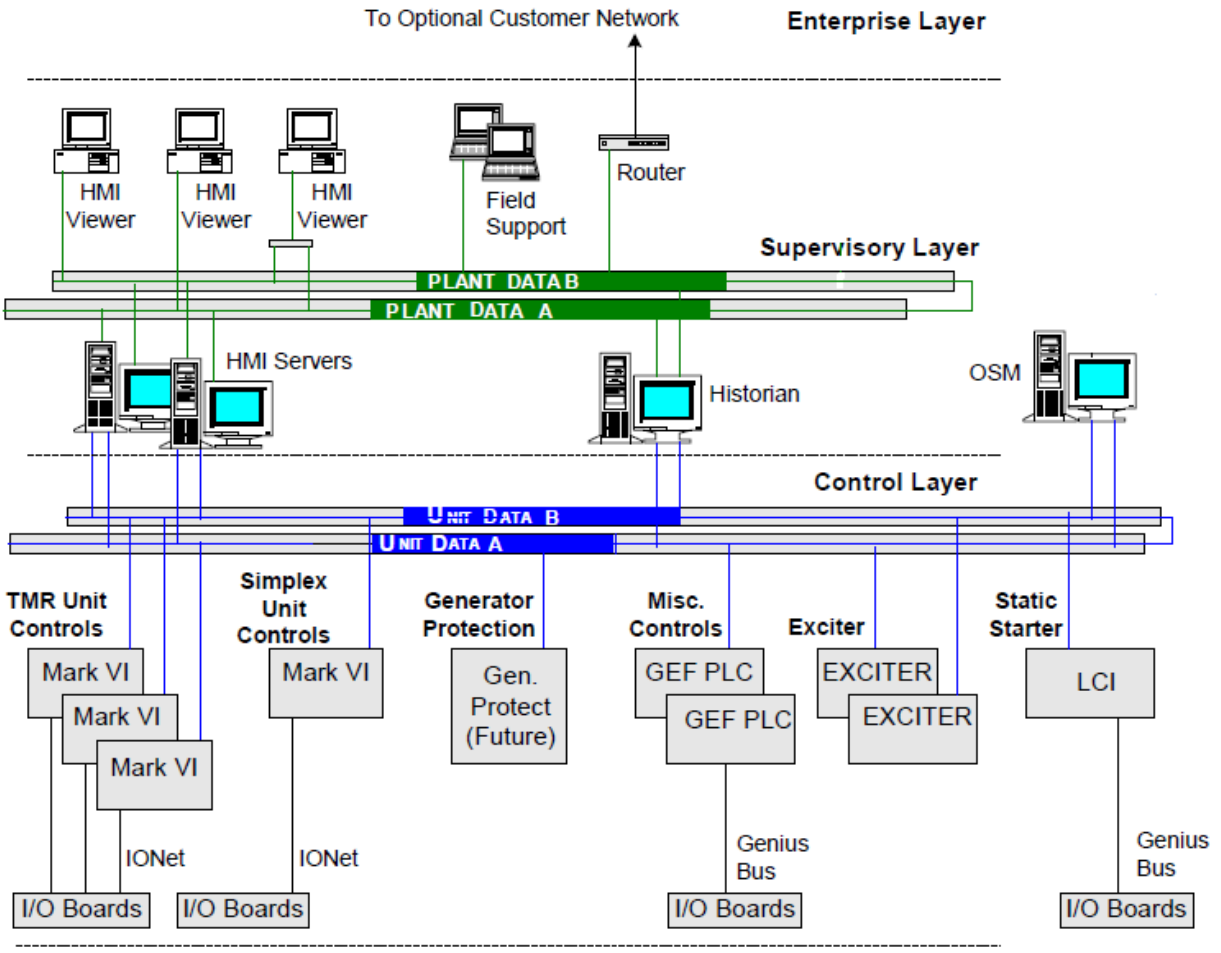


Figure 1: Mark VI network example

Ethernet networks are an integral part of both the Mark VI and Mark VIe product platforms. When developed, these systems were configured with standard Ethernet software services such as FTP and Telnet.

FTP (File transfer protocol) allows for the transmission of data files over the network. Telnet is a very common terminal session program that allows some basic remote interface with a computer or controller over the network. Neither services have inherent security or encryption and transmit any user identifier or password data in plain text format, making this information vulnerable to capture by hackers. In addition, Mark VI and Mark VIe controllers have historically

shipped with simple default passwords, which also increase the chance of unauthorized access. FTP and Telnet may present a concern in the UDH part of the network.

Another potential concern is remote access to the HMI controllers by unauthorized individuals. For the most part, these concerns were identified and mitigated when remote connection and control of the HMI was developed (for remote tuning and diagnostic troubleshooting). However, the same remote access utilities used to provide remote service are a potential vulnerability and it is now recommended to disable these services when not in use.

Finally, this TIL recommends the application of a network traffic filter between the UDH network and any remote network connections (shown as the S3C in lower left of Fig 2). This device will block all non-control related traffic from entering the UDH from an external source such as an OSM. This can provide an additional layer of security within the plant perimeter.

GE will continue to monitor and help customers to improve their security postures and to support compliance efforts as they relate to our equipment.

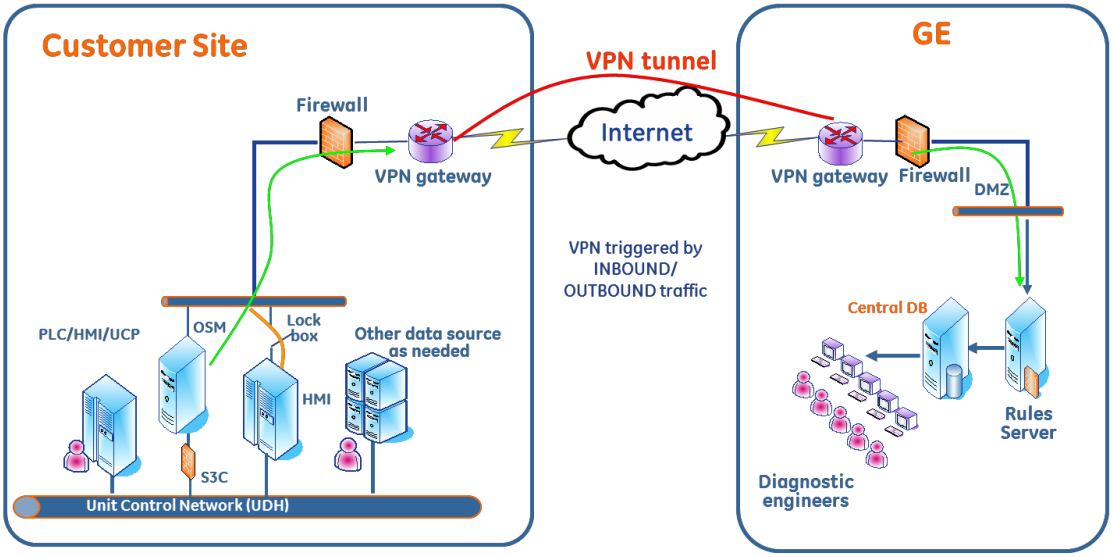


Figure 2: Typical high level overview of plant with OSM and remote tuning capability

Due to the wide range of plant configurations it is necessary to break the recommendations of this TIL down into several sub-parts, some of which may not apply to all systems.

RECOMMENDATIONS

1. **Disable FTP and Telnet services running in the Control Panel**
   This recommendation applies to all sites with Mark VI and VIe platform controllers. These services are not required for normal operation. However they may occasionally be used during maintenance/troubleshooting work and may occasionally need to be temporarily re-enabled. Please see the section titled, "How to Disable Network Services and Modify Passwords in Mark VI and Mark VIe Generation Controllers," in GEH-6808 for detailed instructions on how to disable or re-enable these services. On some HMIs this software tool may have come pre-installed, however if it is not, then it can be ordered using GE part number DS224SVCPATCH01. To determine if it is installed on any particular HMI, search for the following file.

   svc_patch_1.exe

   This software will not run on older Windows™ NT or Windows™ 2000 HMIs. Sites interested in implementing this patch on these systems should contact GE for assistance. This patch will not fix other legacy security vulnerabilities in Windows™ NT or Windows™ 2000 as these products are no longer actively supported by Microsoft (Windows is a trademark of Microsoft Corporation).

2. **Modify the default passwords shipped with the system**
   Customers should modify the default access passwords to the HMIs and control panels and develop a secure but reliable system to manage access to these when necessary. In order to modify the controller default login credentials and password it will be necessary to install the same software patch referenced in recommendation 1. See "How to Disable Network Services and Modify Passwords in Mark VI and Mark VIe Generation Controllers" in GEH-6808 for detailed instructions.

3. **Maintain any remote service lock boxes in the off position when not in use**
   This recommendation only applies to sites with remote tuning (Dry Low NOx tuning) or other remote services capabilities. See appendix B for further details.

4. **Disable HMI remote access software**
   This applies to all sites using HMIs. HMI Remote access software should be disabled. It should be temporarily re-enabled only for approved remote support and disabled again at the end of the support session. NetSupport Manager is the recommended remote access software for all machines in use: pre and post Windows™ 7 HMIs. See appendix C for details on turning on/off these software services.

5. **Install UDH network traffic filtering equipment capable of checking and removing all non- control related traffic**
   This recommendation applies to sites with external network connectivity to the plant control networks. This includes OSM, RSG and customer sites with their own internal remote monitoring and diagnostic systems. More details are provided in Appendix D.

   This TIL can be considered complete when all applicable recommendations have been implemented. For sites without remote connections, that means recommendations 1, 2 and 4 should be implemented. For sites with remote connections to their controller network all 5 recommendations should be implemented.

PLANNING INFORMATION

Compliance

- Compliance Category: **M**
- Timing Code: **6**

Manpower Skills

Controls field engineer

Parts

- HMI software update disk, GE part number DS224SVCPATCH01.
- S3C network filter should be ordered via upgrade process as some site specific configuration is required.

Special Tooling

None required to implement the TIL. However, Mark VI or Mark VIe serial programming cables are required if it is necessary to temporarily re-enable Telnet on the controller. Details and part numbers are provided in GEH-6808.

Reference Documents

- GEH-6808
- TIL 1626 and TIL 1777

Scope of Work

Recommendations 1, 2 and 4 can be implemented in one 8 hr shift for sites with up to 4 HMIs / 4 Control panels and can be implemented by either a Controls field engineer or knowledgeable customer personnel. Recommendation 5 needs to be executed via the upgrade process and once configured may take up to 4 hrs on site to install.

Contact your local GE Service Manager or Contract Performance Manager for assistance or for additional information. Contact your local GE Service Manager or Contract Performance Manager in order to update GE unit record sheets or to submit as-built drawings for changes incurred by this TIL.

APPENDIX A

Recommended Password Protection Guidelines:

These apply to both HMI User passwords (Appendix B) and internal controller passwords (GEH-6808).

At a minimum, the responsible entity shall require and use passwords, subject to the following, as technically feasible:

- Each password shall be a minimum of six characters.
- Each password shall consist of a combination of alpha, numeric, and "special" characters.
- Each password shall be changed at least annually, or more frequently based on risk.

In order for GE remote personnel to authenticate to an HMI after the lockbox is in the closed position, the customer must provide a username and password. It is recommended that HMI passwords comply with minimum length, complexity requirements, and that expiration requirements and account activity are reviewed on a periodic basis. It will remain the customer's responsibility to maintain secure but ready access to the various account details. It is important that proper records of accounts and passwords be maintained by the site as inability to locate this information may result in significant delays to maintenance related activities.

APPENDIX B

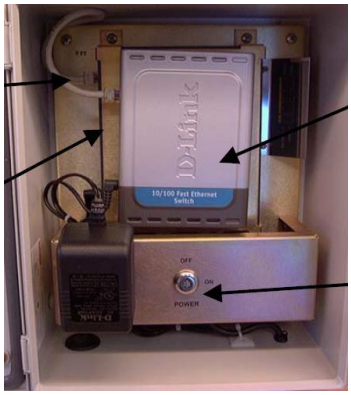


Figure 3: Example Remote Connection Lockbox

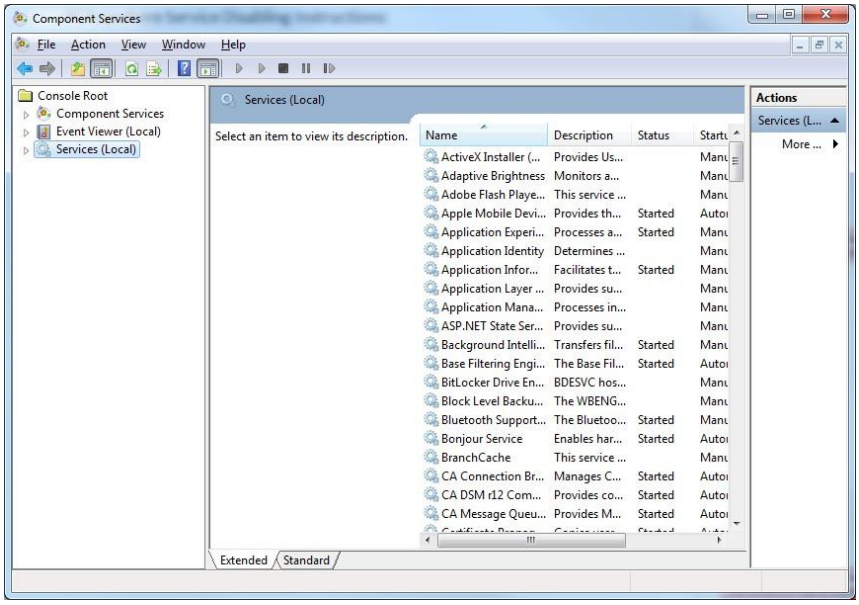
The lockbox is a device that can power up/ down the router which enables access to the HMI via the OSM or in some cases the RSG. The lockbox physically isolates the power to the router that enables this communication pathway and access to both the box and the key should be controlled. In order to reduce disruption to maintenance activity, there should be a secure, well defined process to get this turned on or off as required. When no pre-arranged tuning or diagnostic activity is in progress, it should be in the locked off position.

APPENDIX C

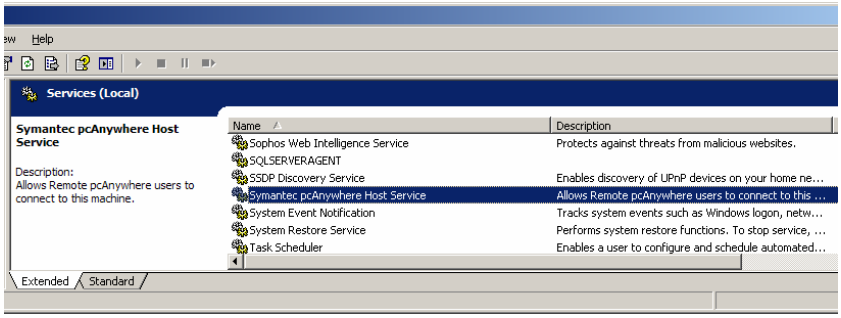
Windows™ 7 and earlier HMIs using PC Anywhere or with PC Anywhere installed from the factory

PCAnywhere Service Disabling Instructions:

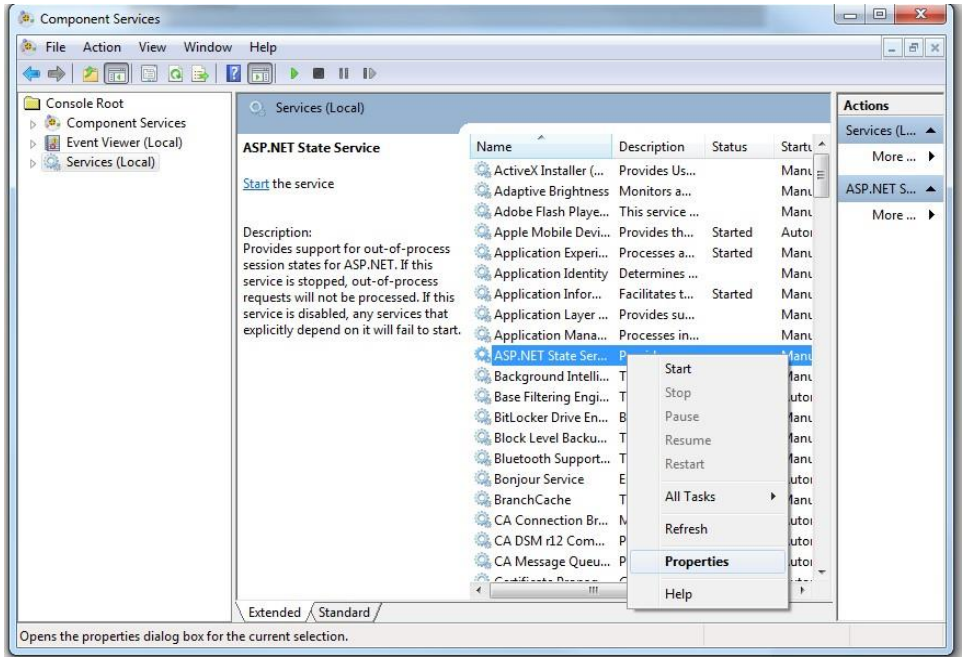
1. Go to "Start" Menu ; Select "Run"
2. On the Run Box type "Services" and hit the "Enter" key. Component Services window will open as shown below. Select "Services (local)" on left panel.



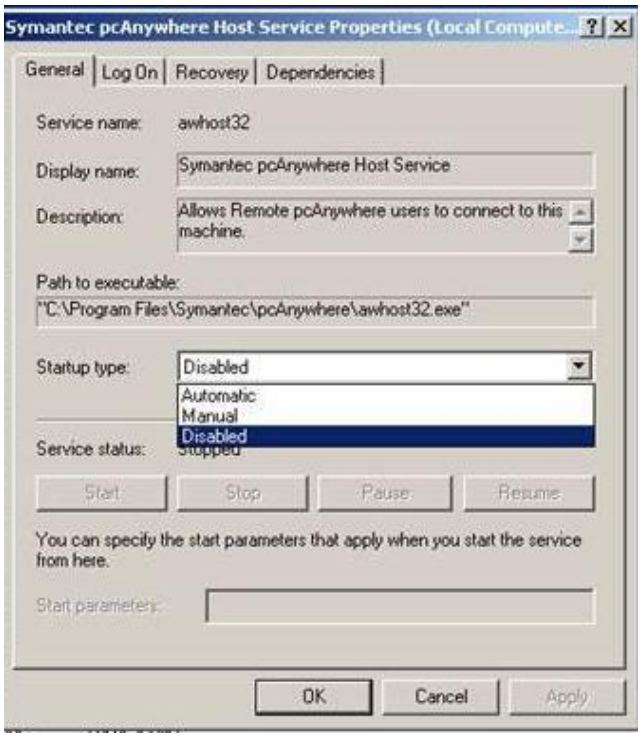
3. Look for “Symantec pcAnywhere Host Service” on right panel and select that service.



4. To disable the service right click and select “Properties”.

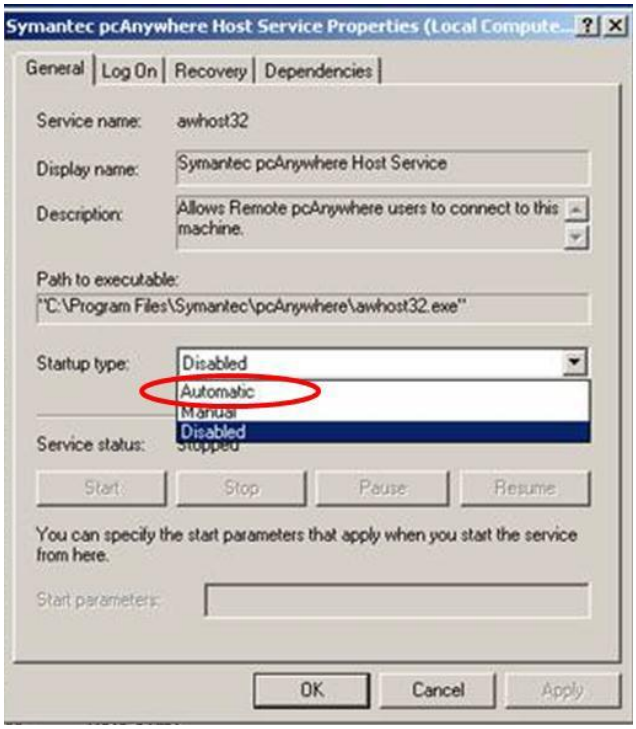


5. Select "Disabled" from Startup type drop down in the Symantec pcAnywhere Host Service Properties window. As shown below. Click OK.



PCAnywhere Service Enabling Instructions:

1. Follow step 1 to 4 as described above instruction set.
2. Select "Automatic" from Startup type drop down in the Symantec pcAnywhere Host Service Properties window. As shown below. Click the Apply button.

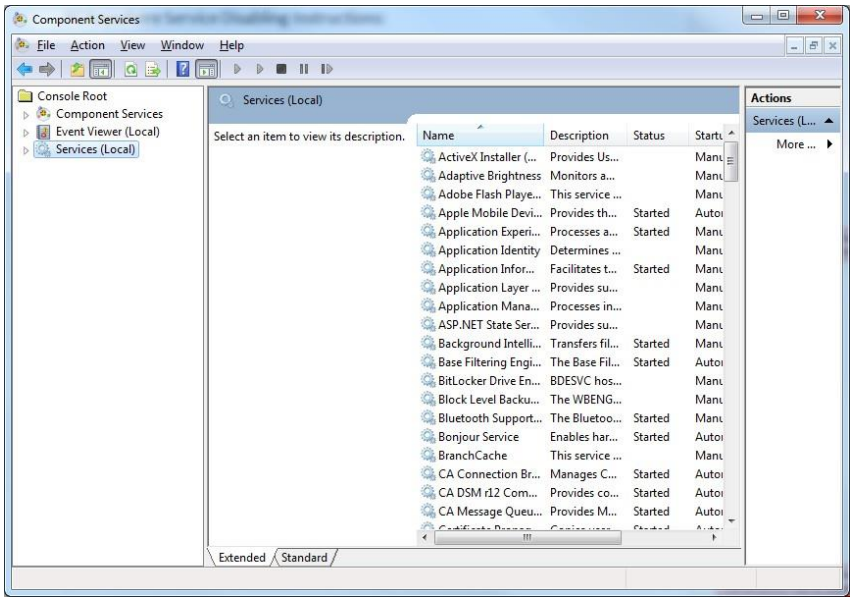


3. Once the service is set Automatic click the Start button to start the service. Click OK.

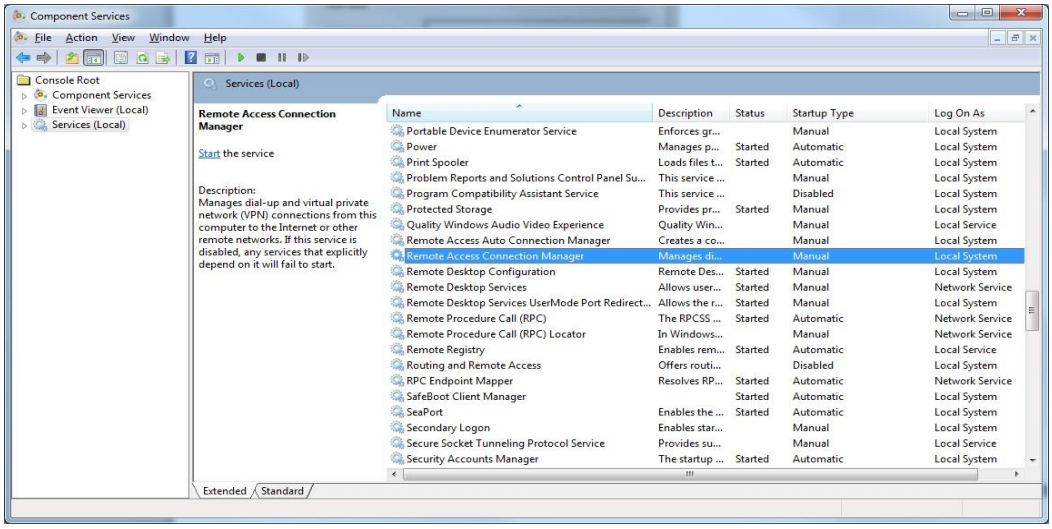
Windows™ XP and 7 HMIs using Microsoft Remote Desktop Connection

Remote Desktop Service Disable Instructions:

1. Go to “Start” Menu ; Select “Run”
2. On the Run Box type “Services” and hit the “Enter” key. Component Services window will open as shown below. Select “Services (local)” on left panel.



3. Look for “Remote Access Connection Manager” on right panel and select that service.

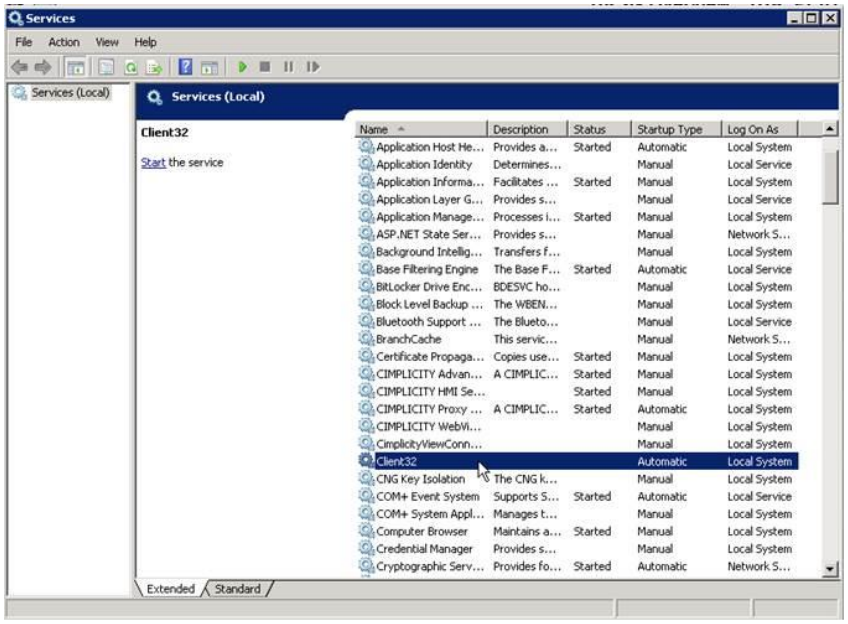


4. To disable the service right click and select “Properties”.

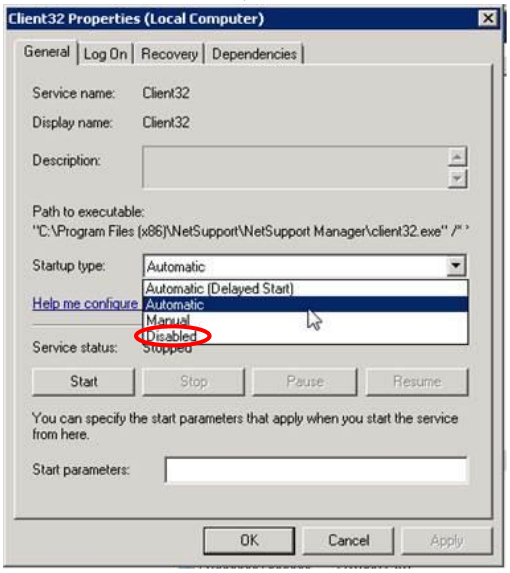
Windows™ XP and 7 HMIs using NetSupport Manager

NetSupport Manager Disable Instructions:

1. Go to “Start” Menu ; Select “Run”
2. On the Run Box type “Services” and hit the “Enter” key. Component Services window will open as shown below. Select “Services (local)” on left panel.
3. Look for “Client32” on right panel and select that service.



4. Right click on the Client32 service and select Properties
5. To disable the service, choose Disabled from the Startup Type list box and click the OK button.



6. To re-enable NetSupport Manager service, follow steps 1-4 and chose Automatic from the Startup Type list box and click Apply. Click the Start button and click OK.

APPENDIX D

S3C (Support segment security connector availability)

This is an optional additional layer of protection to isolate the controller network from unapproved traffic.

Perimeter Protection

Like an Internet Firewall, the S3C is inserted at the edge of your electronic security perimeter on your Unit Data Highway (UDH). It serves as the gateway for ALL traffic between your M&D on-site monitoring equipment and devices within your control system network. The S3C inspects and filters all incoming or outgoing communications required for monitoring or remote tuning of your assets.

Controlled Communication

Only the network communications that explicitly match those permitted by our custom policies will traverse through the S3C, all other communications should be denied and then captured for your review.

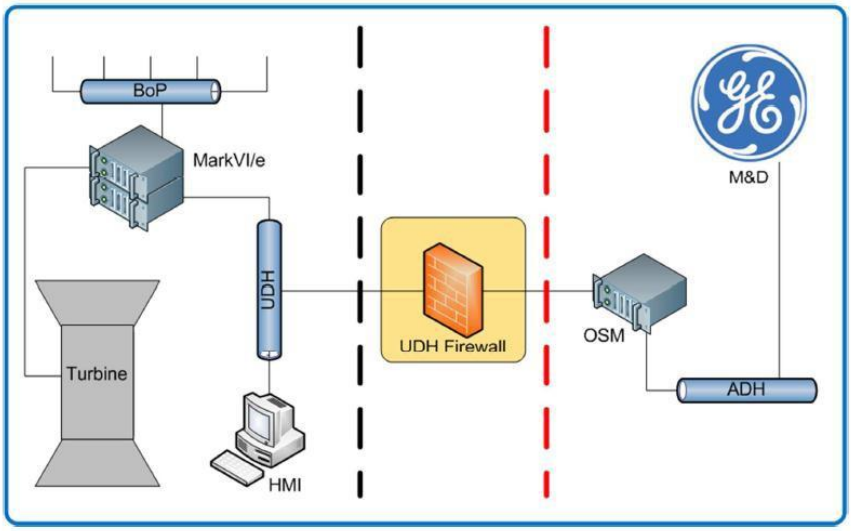


Figure 4: S3C (UDH Firewall) shown inserted between OSM and the UDH

Tiered Inspection: The S3C inspects communications passing between interfaces and evaluates it against multiple criteria established in custom policies specifically tailored for M&D services. Any traffic that does not conform to ALL of the criteria defined within a policy is denied access to its network target.

Permitted Services: Only communications necessary for legitimate functionality and operation of approved resources should be permitted. The S3C provides exactly this level of control. GE security engineers have systematically identified all required communication ports and protocols for M&D services for required functions with their associated resources. These have been documented and authored into the S3C policies to permit these communications.

Cyber Security

The M&D platform is configured to provide customers with a secured data connection helping them to achieve their security compliance requirements. The basis for network security comes down to permitting only what is necessary in order to maintain the performance and operation of required services. GE has created the S3C with an auditable, defensive position to facilitate this.

Security Management

M&D is committed to providing a solution that fits into your enterprise security management. Embedding industry best practices for security management into the S3C allows for a seamless integration into your existing infrastructure and technology administration. We provide security that allows vendor transparency and maintains your independence from external security policies.

Configuration

Some site specific configuration will be required.

Ordering

Because some site specific setup and configuration is required these devices should be ordered via the upgrade process so that the correct site specific parts and configuration can be installed.

Management Features

Independent Management Interface, event Logging, traffic Logging, SNMP Alerts.

TIL COMPLIANCE RECORD

Compliance with this TIL must be entered in local records. GE requests that the customer notify GE upon compliance of this TIL.

Complete the following *TIL Compliance Record* and FAX or Email it to:

TIL Compliance
FAX: (678) 844-3451
Email: til.compreq@ge.com

TIL COMPLIANCE RECORD	For Internal Records Only # _____
Site Name:	Customer Name:
Customer Contact Information	**GE Contact Information**
Contact Name:	Contact Name:
Address:	Address:
Email:	Email:
Phone:	Phone:
FAX:	FAX:
Turbine Serial Number(s):	

INSTALLED EQUIPMENT	TIL Completed Date: _____
	100% TIL Completed: _____
Description:	

Unit Numbers:	Part Description:	Part Number	MLI Number

Comments:

NOTE: *If there are any redlined drawings that pertain to this TIL implementation, please FAX or Email the drawings along with this TIL Compliance Record.*

FAX this form to: **TIL Compliance**
FAX: (678) 844-3451
Email: til.compreq@ge.com