

# Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0268.html>

---

**From:** Patrick Coomans ([Patrick.Coomans@4all.be](mailto:Patrick.Coomans@4all.be))

**Date:** 09/28/01

Message-Id: <sbb4ceb2.077@mail.4all.be>

Date: Fri, 28 Sep 2001 19:25:32 +0200

From: "Patrick Coomans" <[Patrick.Coomans@4all.be](mailto:Patrick.Coomans@4all.be)>

To: <[PEN-TEST@SECURITYFOCUS.COM](mailto:PEN-TEST@SECURITYFOCUS.COM)>

Subject: Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7

Have you already tried launching a DOS attack against an Allen Bradley PLC? I only have Siematic PLC's here with me to play with.

Thx,  
Patrick

>>> "Nasir Farhat Khan" <[nasir@instecdigital.com](mailto:nasir@instecdigital.com)> 28/09/01 07:52 >>>

If the PLC is on TCP/IP you can check whether it supports SNMP. Some of the PLCs use SNMP for management. We have seen Allen Bradley devices popping up with SNMP management turned up on of our pentests.

One more possibility is that you can get hold of the PC programs that are used to program the PLCs i.e. the Loader or Ladder Logic/Graphic programming since most of the PLCs have little or no authentication barriers in terms of login names and passwords you can get hold of the running configuration etc.

IMPORTANT:

DO NOT TO TRY this in a production environment. PLCs are used to control production equipment (machinery) and consequences can be very dangerous and life threatening.

Nasir Farhat Khan  
[nasir@instecdigital.com](mailto:nasir@instecdigital.com)  
Instec Digital Systems – PAKISTAN

[www.instecdigital.com](http://www.instecdigital.com)

----- Original Message -----

## SecurityFocus Penetration: Re: Pen-testing Simatic Data Aquisit

From: "Patrick Coomans" <[Patrick.Coomans@4all.be](mailto:Patrick.Coomans@4all.be)>  
To: ">" <[@securityfocus.com](mailto:@securityfocus.com)> <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>  
Sent: Tuesday, September 25, 2001 11:14 PM  
Subject: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7

I have a project for which I will have to pen-test Siemens PLC's that drive production processes and do data aquisition.

Is there anyone who has literature on this or done this before?

The PLC's use TCP/IP so that will be the first thing I will go for, but most of the PLC's are simply connected to a propriary bus system (e.g. Interbus) which in turn is connected to a PC. So attacking the "Data Aquisition and Visualisation PC" as a backdoor to the PLC would be my second option.

Thanks,  
Patrick

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- **Previous message:** [H D Moore: "Re: BO2k Port?"](#)
- **Maybe in reply to:** [Nasir Farhat Khan: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7"](#)
- **Next in thread:** [Ted Doty: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7"](#)
- **Reply:** [Ted Doty: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7"](#)
- **Reply:** [Nasir Farhat Khan: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5orS7"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)