

# Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 or S7

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0224.html>

---

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

**Date:** 09/25/01

Message-Id: <sbb0e5ae.007@mail.4all.be>

Date: Tue, 25 Sep 2001 20:14:12 +0200

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)>>

Subject: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 or S7

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/>

---

- **Previous message:** [Ockens Thomas: "RE: Web Application Testers."](#)
- **Next in thread:** [Nasir Farhat Khan: "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 S5 orS7"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)