

The image shows two men in business suits standing around a round table, looking at a large document or blueprint. The man on the left is wearing a dark pinstriped suit and an orange tie, while the man on the right is wearing a grey suit and a green tie. They appear to be in a professional setting, possibly a workshop or meeting.

# SIEMENS

## Security Assessment Workshop

# Understanding and implementing industrial security requirements – the safe way

There is no question that industrial plants and their IT systems require reliable protection from both external and internal attacks. This is true today more than ever before and the question you should be asking yourself is: How can I ensure this protection? The first step to achieving security is to inventory, to assess existing and potential risks in your architecture and to recognize sources of these threats. These are exactly the issues which our specially designed workshop deals with. Do not miss this opportunity to find out some great answers!

### **A decisive move towards industrial security**

An important element of our Security Assessment Workshop is to familiarize you with the current IT security requirements and practices for industrial plants. Above all we will show you effective ways and means of reliably eliminating risks – thus ensuring the availability of your production processes in the long term.

As your partner we can offer you a holistic security concept based on the ISA 99 “Industrial Automation and Control Systems Security” requirements. Find out for yourself how you can utilize intelligent and differentiated multi-level protective mechanisms to make sure you always play it safe.



[siemens.com/industrialsecurity](http://siemens.com/industrialsecurity)

# Quick assessment: Contents at a glance

The one-day workshop begins with a general presentation all about industrial security. The following topics are dealt with:

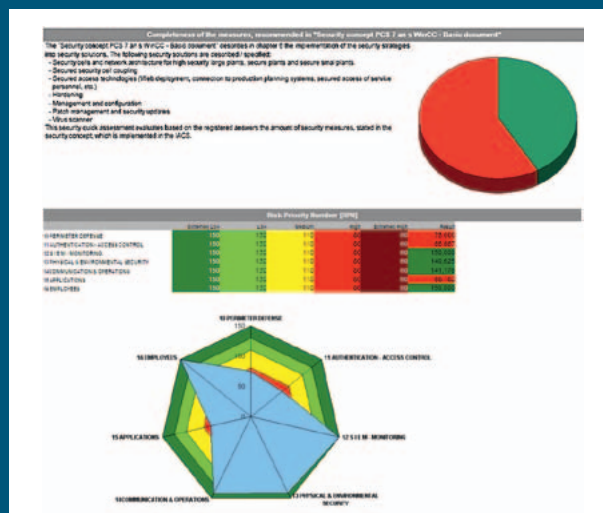
- The increasing significance of Industrial Security (motivation, threat scenarios, norms and standards, legal requirements)
- Strategies for the reliable protection of automation systems
- Introduction to the security concept for the SIMATIC® PCS 7 process control system and the SIMATIC WinCC SCADA system

After the presentation, the safety of a specific automation system is analyzed and potential areas identified which could be improved to achieve better system security. The analysis takes the form of an interview-based assessment attended by your system specialists.



Valuable, real-life information – designed for practical use

The results of the assessment are made available in the form of a written final report. This contains a description of the vulnerable areas identified, as well as suggested measures for eliminating them.



Siemens AG  
Industry Sector  
Industry Automation  
P.O. Box 48 48  
90026 NUREMBERG  
GERMANY

Subject to change without prior notice 09/11  
Order No.: E20001-A1030-P200-X-7600  
Dispo 06303  
SCHÖ/35595 MI.AS.SA.52.1.04 SB 09112.0  
Printed in Germany  
© Siemens AG 2011

The information provided in this brochure contains merely general descriptions or characteristics of performance which in actual case of use do not always apply as described, or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.