ROMAB
ROBERT MALMGREN AB

När Bill släckte ljuset

….eller *vårt ständigt ökade beroende på standardprodukter*

Robert Malmgren

rom@romab.com

+46-708330378

Electronic copies of the slides available at

http://www.romab.com/documents.html

 Copyright © 2008 ROMAB. All rights reserved

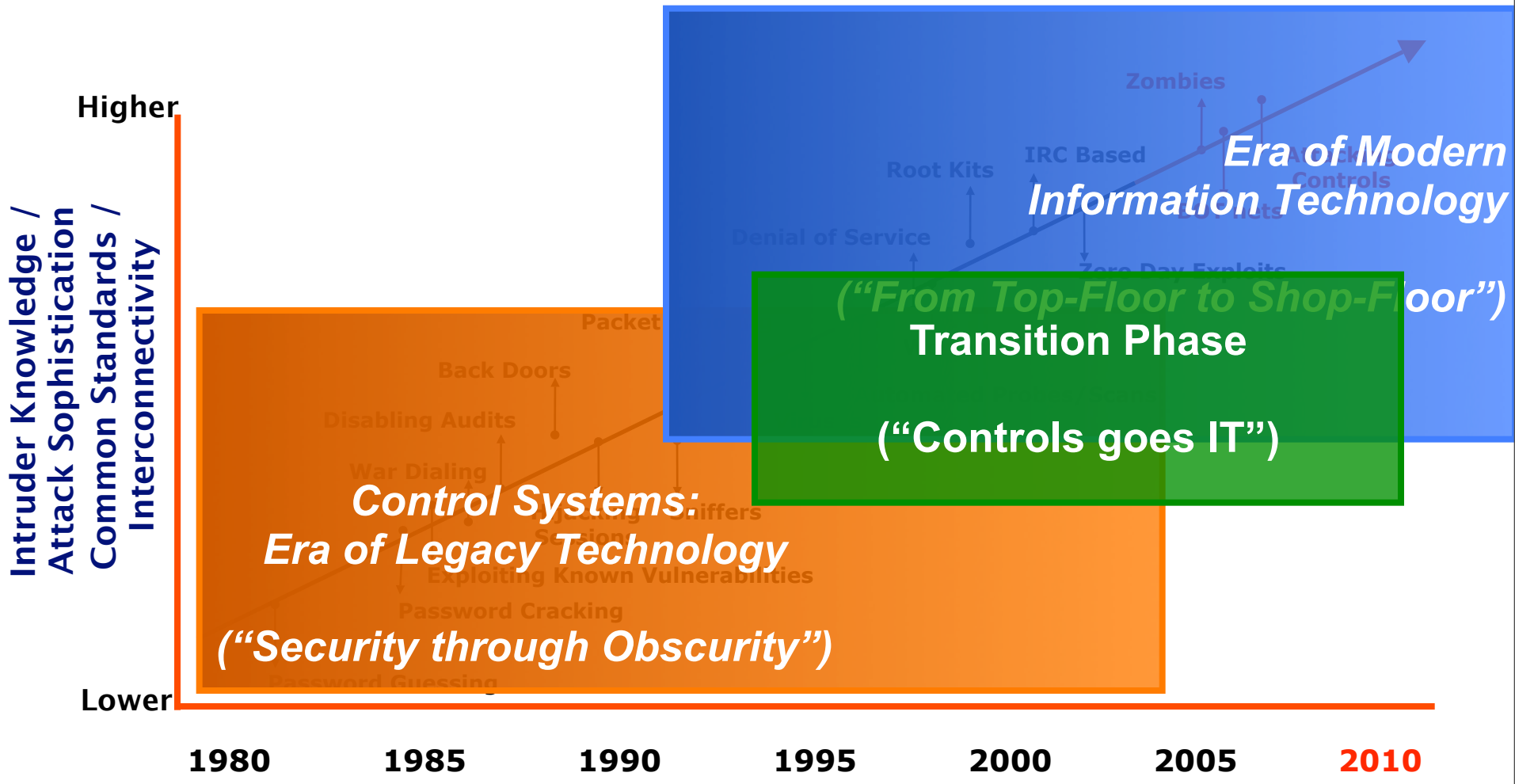
ROMAB
ROBERT MALMGREN AB

Bakgrund

- Energibranschen, som de flesta andra branscher…
  - Automatiserar affären i allt högre grad – automatiserad mätaravläsning, arbetsordrar till handdatorer, etc
  - Integrerar olika IT-lösningar alltmer – skicka data direkt från industri-IT till ekonomi/logistik/ kundhanteringssystem
  - Konvergerar olika kommunikationsvärldar – Larm/ passage/video över TCP/IP, IP-telefoni, Process-IT över kontors-WAN
  - IT-användningen bygger i ökande grad på standardkomponenter – Windows, Linux, office, SAP, etc.

 Copyright © 2008 ROMAB. All rights reserved

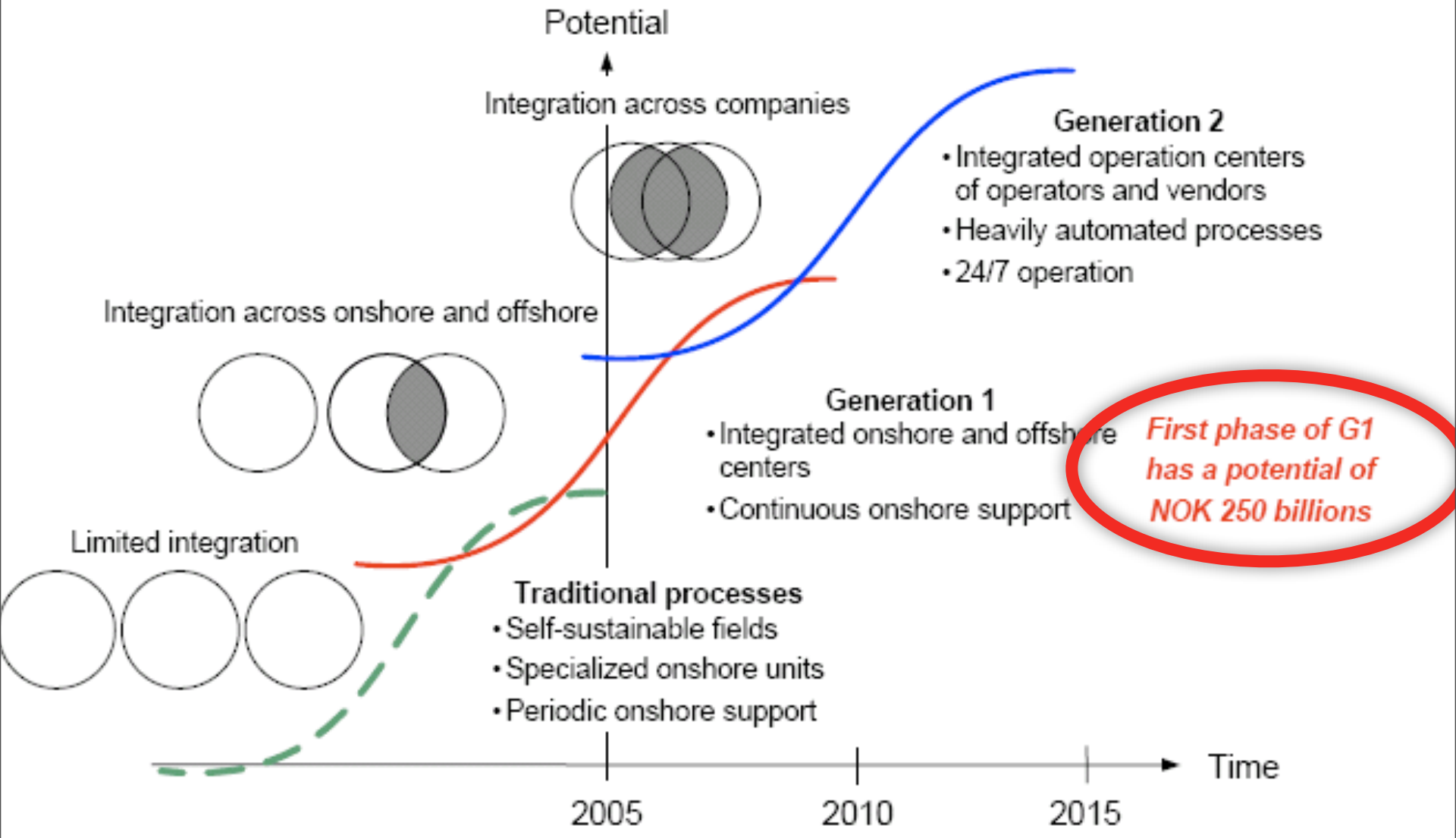
Industrins mognad map IT-säkerhet



Picture borrowed from - Luders, Stefan: Industrial Cyber-Security

 Copyright © 2008 ROMAB. All rights reserved.

Integrated Work Processes
Two future generations



Picture borrowed from -
OLF presentation @ OD, 2006

ROMAB
ROBERT MALMGREN AB

Vad innebär det integrerade företaget?

- Fokus på finansiella rationaliseringsvinster: Spara pengar genom att jobba smartare
  - Fjärrdiagnostik
  - Konstant partnernärvaro
  - Konstant åtkomst för personal m spjutspetskompetens
- Stora krav från användarna på förenklade förfaringssätt
  - Varför manuellt hantera data, och peta in det i flera system, om och om igen...

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Några exempel på vad som gjorts

- Större nordiskt elföretag
  - Praktiska tester i industrimiljö
  - Tester i labbänk
  - Audits av leverantörernas tredjepartsingångar
  - X-jobb för att hitta nya säkerhetsmekanismer och utöka existerande säkerhetskoncept
  - Audits och säkerhetskontroller av anläggningar
  - Framtagande av interna styrdokument och säkerhetsmodeller

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Fältstudie 1 - detaljer

- Det finns bara “*ett system*”
  - Det installerade produktionssystemet
- Opatchade operativsystem, opatchade subsystem och applikationer
- Konstiga applikationer pålagda, onödiga applikationer ligger kvar...
- Konstig nätverksinfrastruktur - “gateway” för att konvertera mellan IEC 104-protokoll och lösningsinterna protokoll

 Copyright © 2008 ROMAB. All rights reserved

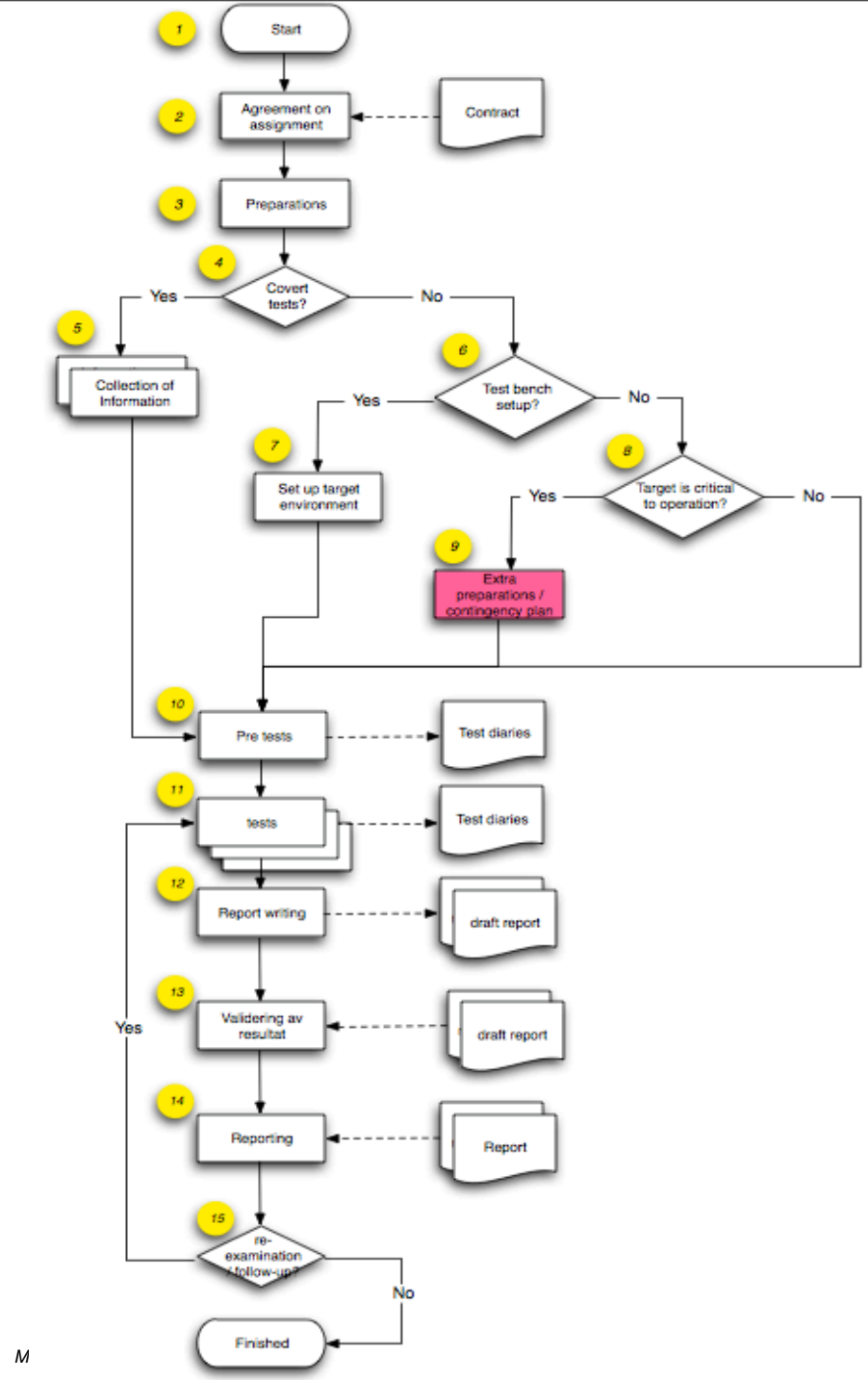
ROMAB
ROBERT MALMGREN AB

Fältstudie 1 - slutsatser

- Skall säkerhetstesterna utföras, måste de göras i det produktionssatta systemet => Ökad risk för driftstörningar
- Går att hacka vitala komponenter med standardverktyg på några få minuter
- De interna nätverkstjänster exponerades via “gateway”-datorn
- “Gatewaydatorn” hade inte någon brandväggsfunktionalitet. Den var dessutom kortsluten pgr av den konstiga nätverksstrukturen
- I princip allt använde samma lösenord - från operatörskonsol, SCADA-applikationerna, switchar,
- Defaultlösenord i databasen

 Copyright © 2008 ROMAB. All rights reserved

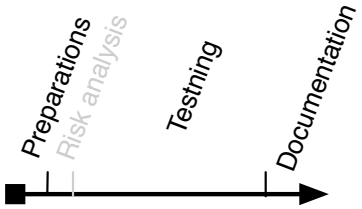
ROMAB
ROBERT MALMGREN AB



ROMAB
ROBERT MALMGREN AB

Pen test methodology

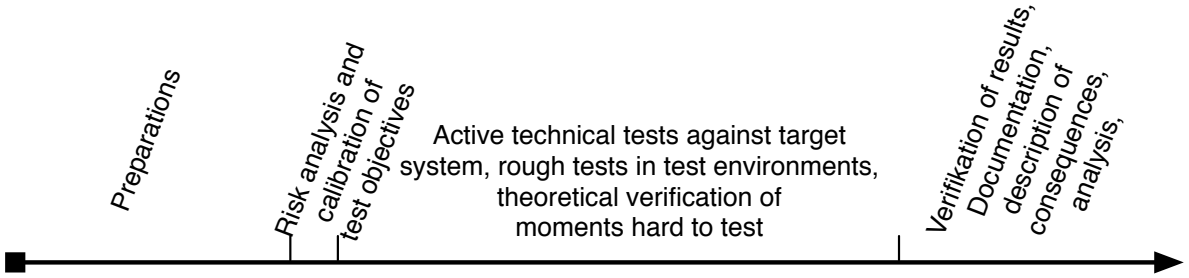
Traditional "pen test"



Normally short assignments

Focus is on producing a fat report with many findings

Adapted "pen test"



Focus on aquiring process & business knowledge -> more adequate results

More time spent with key persons -> more ideas for test cases, better understanding

Testplan & objectives focused on shared understanding of risks, vulnerabilities & threats

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Slutsatser (1)

- Leverantörerna är inte på den kunskapsnivå man kunde förvänta sig
  - 5-10 års eftersläpning jmf IT-sektor
- Många leverantörer har påbörjat initiativ map säkerhetsförbättrande åtgärder
  - Läpparnas bekännelser -> slide ware och marknadsmaterial?

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Slutsatser (2)

- Vi användare är inte på den nivå man kan förvänta sig
  - Dåliga kravställare – Otydliga och inte tillräckligt långsiktiga. Inte heller några gemensamma standard krav (NERC CIP / Procurement language undantag)
  - Dålig kompetens

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Rekommendationer (1/4)

- Försäkra er om att sponsorn och testteamet vet vad som står på spel, tex vilka risker och vilka konsekvenser som det kan bli

- Försäkra er om att målet med testerna är definierade och att alla i projektet vet om dessa innan man startar med jobbet

MELANI meeting 24th May 2008. Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Rekommendationer (2/4)

- Dubbelkolla katastrofplanen innan
  - finns det reservdelar? fungerar den senaste backupen att återläsa från? finns leverantören tillgänglig under testtillfället?
- Försök att hitta och använda de minst riskfyllda testuppsättningarna/ inställningarna
  - Köra testerna mot slavservern? Går det att aktivera något ofarligt “debuggläge”? etc

MELANI meeting 24th May 2008. Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Rekommendationer (3/4)

- Ta leverantörens tekniker på plats under själva testen för frågor, snabba åtgärder, etc
- Ha verksamhetsrepresentant på plats
- Var säker på att dokumentationen ni skapar är övertydlig och vattentät
  - Nätverksdumpar, videoinspelningar av datorskärmar och testaraktiviteter

MELANI meeting 24th May 2008. Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Rekommendationer (4/4)

- Viktigt att utföra uppstädning och återställande till normalläge efter utförd test
  - Se till att testverktyg inte lämnar något kvar, eller att mål för testerna inte blir hängande eller i något konstigt exekveringstillstånd
  - Detta ***kräver sannoligt*** omstarter och nedtid för system, noder eller programkomponenter

MELANI meeting 24th May 2008. Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Still people rely on the *obscurity* factor

Loading "plc, plc software, siemens plc, allen bradley items at low prices on eBay.co.uk"

http://search.ebay.co.uk/search/search.dll?from=R40&_trksid=m37&satitle=plc

post to del.icio.us | my del.icio.us | Send to Pukka | Soekris on O...ng Diskless | Positive Ath... Quotations | Data Visuali... Approaches | nwsmp - tech+bus+world | newsmap

Get It Fast items
Completed listings
Items listed as lots
Item condition
New items only
Listings
Ending within
1 hour
Items priced
to
Show Items
Customise options displayed above.

Related Guides
Trading standards gu...
New to Collecting Cl...
See all related guides...

Matching eBay Shops
Himark Technology (2)
softwarepromotions (2)
BioTekNik Computer Science (1)
the real engineers store (1)
See all matching Shops
See all common keywords

ADVERTISEMENT
with eBay & PayPal
Find out how!

FULL PLC TRAINING SOFTWARE PACKAGE AND GREAT TUTORIALS	Buy It Now	£3.99	Free	P	21h 34m
Bearing Assembly Machines - PLC/automated.	- Buy It Now	£700.00 £2,000.00	£100.00	P	1d 02h 53m
Sanyo PLC 355MB LCD Video/Data Professional Projector Sanyo PLC 355 MB LCD Video/Data Professional Projector (Enlarge)	-	£195.00	£29.99	P	1d 03h 32m
Sanyo PLC-XU41 Projector	4	£13.70	£14.99	P	1d 09h 37m
Mitsubishi F2-20 GF1 + SC-03 PLC Interfaces F1 F2 PLC s	1	£99.00	£5.00	P	1d 12h 43m
Allen Bradley Micrologix 1000 PLC (1761-L32BBB)	3	£26.50	£4.00	P	1d 12h 59m
Sanyo PLC-XU75 Projector MULTIVERSE	-	£150.00	£8.00	P	1d 13h 04m
Siemens PLC ASi 3RK1408 pnuematic valve New (Simatic)	-	£15.00	£6.00	P	1d 13h 36m
Complete PLC Programmable Logic Controller Training	- Buy It Now	£0.99 £3.99	£1.99	P	1d 13h 42m
MITSUBISHI PLC HMI E 300 GRAPHIC / TEXT OPERATOR PANEL BRAND NEW IN BOX WITH MANUALS	8	£250.00	£6.85	P	1d 14h 12m
PLC PROGRAMMABLE LOGIC CONTROLLER TRAINING SOFTWARE CD	Buy It Now	£3.99	£1.00	P	1d 17h 16m
Sanyo PLC-XW20 Multimedia Projector	-	£50.00	£15.99	P	1d 17h 30m
Schneider Modicon Premium Plc System 136 Input / 128 Output, Motion Control, Ethernet etc	Buy It Now or Best Offer	£1,500.00	£25.00	P	1d 18h 29m
Schneider Modicon Premium Plc System 160 Input / 144 Output, Motion Control, Ethernet etc	Buy It Now or Best Offer	£1,500.00	£25.00	P	1d 18h 30m

 Copyright © 2008 ROMAB. All rights reserved

ROMAB
ROBERT MALMGREN AB

Still people rely on the *obscurity* factor

LAPTOP WITH PLC/HMI/SCADA COMMISSIONING MACHINE on eBay, also...Business, Offic

http://cgi.ebay.co.uk/ws/eBayISAPI.dll?ViewItem&ssPageName=STRK:MEWA

post to del.icio.us | my del.icio.us | Send to Pukka | Soekris on O...ng Diskless | Positive Ath... Quotat

View larger picture

Winning bid:	£720.00
Ended:	04-Mar-08 14:48:45 GMT
Postage costs:	To Sweden – Not specified
Post to:	United Kingdom
Item location:	Birmingham, West Midlands, United Kingdom
History:	4 bids
Winning bidder:	6890chapman (242 ☆)
You can also:	Email to a friend

Listing and payment details: Show

Description (revised)

Item Specifics

Condition: **Used**

Dell inspiron 3800 renowed for its super stable operation in the workplace and in the field

Comes with windows 2000 and all the following PLC Automation software fully installed and acti

- Allen Bradley RSLOGIX 500
- Allen Bradley RSLOGIX 500 trainer
- Allen Bradley RSLOGIX 500 Emulate
- Allen Bradley RSLOGIX 5
- Allen Bradley RSLOGIX 5000 Enterprise "The expensive one"
- Allen Bradley RSLOGIX 5000 trainer
- Allen Bradley RSLOGIX 5000 Emulate
- Allen Bradley RSLINX full version not lite version
- Allen Bradley panel builder 32 hmi software
- Allen Bradley RSView 32 supervisor edition with 100K tags
- Allen Bradley RSView studio enterprise
- Allen Bradley Automated desktop
- Allen Bradley Fieldbus
- Allen Bradley Ladder 5
- Allen Bradley Ladder 500
- Allen Bradley RSMacc
- Allen Bradley control flash upgrade software

LAPTOP WITH PLC/HMI/SCADA COMMISSIONING MACHINE on eBay, also...Business, Office Industrial (end time 04-Mar-08 14:48:45 GMT)

http://cgi.ebay.co.uk/ws/eBayISAPI.dll?ViewItem&ssPageName=STRK:MEWAX:IT&item=2602

post to del.icio.us | my del.icio.us | Send to Pukka | Soekris on O...ng Diskless | Positive Ath... Quotations | Data Visuali... Approaches

- Fuji FLEX_PLC
- Nais FPSOFT
- Full CITECT SCADA package including runtime and work licence
- Kepware
- Mac 50 software for misubishi HMI "older version"
- E-designer for Mitsubishi HMI "new versions"
- Mitsubishi HMI tools
- Mitsubishi remote access View
- Mac programmer plus for mac 10 mac 50 mac 90 etc
- Mitsubishi Melsec GX developer
- Mitsubishi GX simulator
- Mitsubishi GT works GOT HMI range
- Siemens logo
- Toshiba TCPRGROS
- Toshiba TSPC robot software
- Zelio
- Crouzet millennium
- Gmwin for LG and IMO plc
- Idec WINDLR
- Idec WINDLGC
- Idec Wind I/O-Nv
- Omron syswin plc
- Omron sysdrive
- Siemens Prodave S7
- Mitsubishi programming manuals
- Mitsubishi books

Plus full IEE 16th edition test and inspection software and certificate printing software forms etc.

CableCalc Pro wiring and distribution software and certification software that covers from substation to end of line with fuse breaker sizing cable

Include the award winning AUTOMATION STUDIO software for full design and test of almost any project

Also CADDY+ software for wiring and documentation manuals etc.

Turbofast Cad software and some automotive software and tools.

ROMAB
ROBERT MALMGREN AB

Mer information

- KBM / FIDI-SC skrift om *IT-säkerhet och industri-IT*
  - Engelsk & svensk bok under tryckning
- http://www.digitalbond.com
- *Scada security & critical infrastructure protection* öppen engelskspråkig e-postlista
  - Skicka mail till rom@romab.com
- E5, Öppen svensk e-postlista mer policyinriktning
  - Skicka mail till rom@romab.com
- Sec-heads, Stängd engelskspråkig e-postlista inriktad mot avancerade tekniska frågor. 150+ medlemmar
  - Skicka mail till rom@romab.com

 Copyright © 2008 ROMAB. All rights reserved