Erno Pentzin

Protecting an Industrial AC Drive Application against Cyber Sabotage

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 2013-01-28

Thesis supervisor:

Asst. Prof. Marko Hinkkanen

Thesis instructor:

M.Sc. (Tech.) Mika J. Kärnä

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Erno Pentzin

Title: Protecting an Industrial AC Drive Application against Cyber Sabotage

Date: 2013-01-28 Language: English Number of pages:15+119

Department of Electrical Engineering

Professorship: Electric Drives Code: S3016

Supervisor: Asst. Prof. Marko Hinkkanen

Instructor: M.Sc. (Tech.) Mika J. Kärnä

Discovered in 2010, the highly advanced computer virus called Stuxnet, also described as the first weapon of cyber warfare, reportedly destroyed at least 1,000 gas centrifuges enriching uranium in Iran. This kind of act of cyber sabotage was conducted by compromising the industrial control system, disabling protection functions of AC drives running the centrifuges, and making them spin at such high speeds that centrifugal forces caused their rotors to rupture.

Decanters are another type of centrifuges used to separate solids from liquids in many industries including water treatment and mining for example. Also known as solid-bowl, scroll-discharge centrifuges, decanters are commonly powered by induction motors and AC drives. Assuming havoc similar to the Stuxnet case can be prevented with suitable safety systems, a review was conducted on the protection methods for decanter centrifuges based on literature and the current security and safety features of the following modern AC drives with Ethernet-based fieldbus connectivity: ABB ACS880-01, Rockwell Allen-Bradley PowerFlex 755, and Siemens SINAMICS S110.

As a result of the limited assessment, the worst vulnerability related to cybersecurity of the AC drives is typical to many automation devices using fieldbuses: total configuration is possible remotely without any authentication by default. However, the functional safety configuration can be protected by means of a password, therefore allowing a standardized safety function called safely-limited speed (SLS) to become a viable solution for protecting the decanter centrifuge against cyber sabotage. By following the supplied checklist, it is possible to configure AC drives used with decanters optimally in terms of cybersecurity.

Keywords: industrial, AC drive, cyber, sabotage, Stuxnet, decanter, centrifuge, Ethernet, safety, security, cybersecurity, ICS, SCADA, automation, fieldbus, functional safety, frequency converter, induction motor

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Erno Pentzin

Työn nimi: Teollisen taajuusmuuttajasovelluksen suojeleminen kybersabotaasilta

Päivämäärä: 2013-01-28 Kieli: Englanti Sivumäärä:15+119

Sähkötekniikan laitos

Professuuri: Sähkökäytöt Koodi: S3016

Valvoja: Professori Marko Hinkkanen

Ohjaaja: DI Mika J. Kärnä

Vuonna 2010 havaittua, erittäin kehittynyttä tietokonevirusta nimeltä Stuxnet on kuvailtu myös ensimmäiseksi kybersodan aseeksi, koska eri lähteiden mukaan se tuhosi vähintään 1 000 uraania rikastavaa kaasusentrifugia Iranissa. Tämä kybersabotaasi suoritettiin tunkeutumalla teolliseen ohjausjärjestelmään, kytkemällä sentrifugeja ohjaavien taajuusmuuttajien suojatoiminnot pois päältä ja pyörittämällä niitä niin suurilla nopeuksilla, että keskipakoisvoimat aiheuttivat roottoreiden repeämisen.

Dekantterit ovat toisenlaisia sentrifugeja, joita käytetään erottamaan kiinteät aineet nestemäisistä useilla eri teollisuudenaloilla, kuten esimerkiksi vedenkäsittelyssä ja kaivostoiminnassa. Dekantterisentrifugit, eli tarkemmin kiinteärumpuiset, ruuvipurkuiset lingot, käyvät usein epätahtikoneilla ja taajuusmuuttajilla. Olettaen, että Stuxnet-tapauksen kaltainen tuho voidaan estää sopivilla turvajärjestelmillä, toimenpiteitä dekantterilingon suojelemiseksi tutkittiin käyttäen kirjallisuutta ja nykyistä tietoturva- ja henkilöturvaominaisuustarjontaa seuraavilta uudenaikaisilta taajuusmuuttajilta, joissa on Ethernet-pohjainen kenttäväyläyhteys: ABB ACS880-01, Rockwell Allen-Bradley PowerFlex 755 ja Siemens SINAMICS S110.

Rajoitetun arvioinnin tuloksena taajuusmuuttajien pahin kyberturvallisuuteen liittyvä haavoittuvuus on tyypillinen monille kenttäväyliä käyttäville automaatiolaitteille: täysivaltainen asetusten muutos on mahdollista oletusarvoisesti ilman minkäänlaista käyttäjähallintaa. Kuitenkin toiminnallisen turvallisuuden asetukset voidaan suojata salasanalla, joten standardoitu turvafunktio nimeltä turvallisesti rajoitettu nopeus on toteuttamiskelpoinen ratkaisu dekantterilingon suojelemiseksi kybersabotaasilta. Liitteenä olevaa tarkistuslistaa seuraamalla dekanttereissa käytettävät taajuusmuuttajat voidaan konfiguroida mahdollisimman hyvin kyberturvallisuuden kannalta.

Avainsanat: teollinen, taajuusmuuttaja, kyber, sabotaasi, kybersabotaasi, dekantteri, sentrifugi, linko, turvallisuus, tietoturva, kyberturvallisuus, automaatio, kenttäväylä, toiminnallinen turvallisuus

Preface

This thesis was made for the ABB Drives Helsinki factory (FIDRI) during the time period between July, 2012, and January, 2013. It would not have been possible without the support of certain individuals, for who I wish to express my gratitude now.

Firstly, I would like to thank Mr. Janne Henttonen and Mr. Tuomo Höysniemi of LAC R&D for arranging prosperous working conditions for me. Without their support, I could have not been able to work to my fullest extent on my thesis.

Secondly, I have greatly appreciated the most valuable support of my instructor Mr. Mika J. Kärnä of ABB Drives, and supervisor Mr. Marko Hinkkanen of Department of Electrical Engineering of Aalto University. I want to express my gratitude to those two gentlemen for their time spent reading my drafts and the excellent feedback provided.

Thirdly, my thanks to Mrs. Marjukka Patrakka and Mr. Janne Vuori of Department of Materials Science and Engineering of Aalto University for co-operation in providing a highly important source material for me. Without it, my knowledge of decanter centrifuges would be substantially less. Also the following persons made crucial contributions for which I am grateful: From ABB Drives, Mr. Timo Holttinen for providing his valuable decanter expertise, Mr. Petteri Ämmälä and Mr. Petri Torniainen for product expertise, and Mr. Mikko Ristolainen for functional safety resources. And from PLABB, Mr. Dawid Piech and Mr. Janusz Maruszczyk for standards resources.

Then, my thanks to the following co-workers from ABB Drives in no particular order: Juho for organizing *Tmnttrst* events regularly for the benefit of employee satisfaction, Pasi for participating these events regularly for good company, Heikki for daily lunch plans and testing support, Lauri K. for coffee break reminders and fitness exercise company, Olli A. and Olli V. for LaTeX support, Ville for providing practical tips about thesis making, Vassili for fruitful conversations, Jyri for lunch company, Jarmo T., Markku S., Micke, Matti V., Petri M., and Markku J. for interesting aisle conversations, and for all other ABB colleagues who I forgot to mention. Special acknowledgment goes to Hard Test Café regular crew for providing answers to any question imaginable by mankind.

I would also like to thank Mrs. Päivi Palm and others from Helsinki Polytechnic (Stadia) who encouraged me to continue my studies. Remembering my time in that school brings the following quote to my mind:

> "you can't connect the dots looking forward;
> you can only connect them looking backwards." —Steve Jobs (2005)

My studies have taken time, but some wise person has once said that the journey is more important than the destination. I could not agree more.

In addition, I would like to thank the individuals, teams, organizations, and corporations behind the following free tools and applications I have used for making this thesis: Firstly, the most important tools, my cross-platform "trusted trio" consisting of LaTeX 2_ε, TeXstudio, and JabRef. Then, in no specific order: MiKTeX,

MacTeX, Dropbox, Workrave, Dia, and a bunch of LaTeX packages. Those tools have enabled me to work as efficiently as I have could.

Also, the following websites have been a big help for me: The Purdue University Online Writing Lab (`http://owl.english.purdue.edu/`) for helping me navigate through the English grammar, and TeXample.net for LaTeX example code.

And while speaking of things which have helped me, I must mention music as a major contributor (and sometimes even enabler with ambient noise reducing headphones). Thanks to Aphex Twin (Richard David James) for his spectacular *Selected Ambient Works 85-92* album which has helped me in the creation process of this thesis. Also a big help in sinking into the state of flow has been GetWorkDoneMusic.com, introduced to me by Lifehacker (`www.lifehacker.com`). And *Electronic Architecture 2* album by Solarstone (Richard Mowatt), *D. Trance 6* album by Gary D. (Gerald Malke), and many others.

I've enjoyed working on this thesis combining power electronics, electric drives, cybersecurity, and even nuclear physics and world politics. During this time which I have spent studying all these wonderful things, I have had the same of kind of feeling as in this next quote:

> "For the world is changing:
> I feel it in the water,
> I feel it in the earth,
> and I smell it in the air."
> —Treebeard / J. R. R. Tolkien: *The Return of the King* (1997)

Finally, I want to thank my beloved wife Mimmi for each day I have had the privilege to spent with her. This thesis is dedicated to our first child, whose quickly forthcoming due date has been the greatest motivator for me.

Helsinki, January 28, 2013

Erno Pentzin

Contents

Symbols and Abbreviations

Symbols

Latin Letters

a	Acceleration
D	Diffusion coefficient
f	Frequency of the line voltage
f_N	Nominal frequency of an electric machine
g	Gravity on Earth (≈ 9.81 m/s^2)
g_c	Ratio of centrifugal acceleration to the gravity (g-level)
I_{max}	Maximum output current of a drive
I_N	Nominal current of a drive or an electric machine
l	Length
m_{GB}	Gearbox ratio
ΔM	Molecular weight difference
n	Asynchronous speed
n_{bowl}	Bowl speed
n_d	Differential speed (of the conveyor)
n_N	Nominal speed of an electric machine
n_p	Gearbox pinion speed
n_s	Synchronous speed
O	Solids recovery
p	Number of pole pairs
P_M	Power on the motor shaft
P_N	Nominal power of an electric machine
Q_f	Flow rate of the feed
Q_l	Flow rate of liquids
r	Radius
R	Universal gas constant (≈ 8.3 J/mol K)
s	Slip of an induction motor
T	Temperature
T_c	Conveyor torque
T_N	Nominal torque of a motor
T_p	Pinion torque
U_N	Nominal voltage of an electric machine
v	Velocity
v_a	Peripheral velocity
ΔW	Separative work unit (SWU)
x_f	Fraction of solids in the feed
x_l	Fraction of solids in the centrate (liquids)

Greek Letters

$\cos\varphi$	Cosine of the angle between current and voltage, i.e. percentage of apparent power S used as active power P
η_B	Efficiency of a belt coupling
η_F	Efficiency of a fluid coupling
ρ	Density
ρ_f	Density of the feed
ρ_l	Density of the centrate (liquids)
ω	Angular velocity
ω_m	Electrical angular velocity of the rotor

Abbreviations

3G	3rd Generation
AB	Allen-Bradley (or *AktieBolag*, Swedish for incorporated company, Inc.)
AC	Alternating Current
AG	*AktienGesellschaft* (German for incorporated company, Inc.)
AM	Asynchronous Machine
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
Auto-MDIX	Automatic Medium Dependent Interface crossover
AWL	Application WhiteListing
BBS	Bulletin Board System
BOOTP	BOOTstrap Protocol
BSD	Berkeley Software Distribution
C&C	Command and Control (server)
CA	Certificate Authority
CCW	Connected Components Workbench
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection (with NERC, see below)
CIP	Common Industrial Protocol (with EtherNet/IP)
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CU	Control Unit
D2D	Drive-to-Drive (link)
DC	Direct Current
DDS	Drive Data Set
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIN	*Deutsches Institut für Normung* (German Institute for Standardization)
DLL	Dynamic Link Library

DMZ	DeMilitarized Zone
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DP	Decentralized Peripherals (as in PROFIBUS DP, see below)
DPI	Drive Peripheral Interface
DRIVE-CLiQ	DRIVE-Component Link with iQ
DTC	Direct Torque Control
e.g.	*exempli gratia* (Latin for "for example")
e.V.	*eingetragener Verein* (German for registered association)
E/E/PE	Electrical/Electronic/Programmable Electronic
EEPROM	Electronically Erasable Programmable Read-Only Memory
EnDat	Encoder Data (interface)
ERP	Enterprise Resource Planning
ESP	Electronic Security Perimeter
et al.	*et alii* (Latin for "and others")
etc.	*et cetera* (Latin for "and so on")
EU	European Union
EUC	Equipment Under Control
FBA	FieldBus Adapter
FBI	Federal Bureau of Investigation
FCS	Frame Check Sequence
FEP	Fuel Enrichment Plant
FTP	File Transfer Protocol
GmbH	*Gesellschaft mit beschränkter Haftung* (German for LLC, see below)
GIMP	GNU Image Manipulation Program
GNU	GNU's Not Unix
GPL	General Public License
GTK	GIMP ToolKit
GUI	Graphical User Interface
HEU	Highly Enriched Uranium
HMI	Human-Machine Interface
HTL	High Threshold Logic
HTTP	HyperText Transfer Protocol
I/O	Input/Output
IACS	Industrial Automation and Control System
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ID	IDentification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
IEA	International Energy Agency
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Device
IGBT	Insulated Gate Bipolar Transistor
IM	Induction Motor
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Information Security
ISA	International Society of Automation
ISO	International Organization for Standardization
ISO-TSAP	ISO Transport Service Access Point (protocol)
ISIS	Institute for Science and International Security
IT	Information Technology
ITU	International Telecommunication Union
L/D	Length to Diameter (ratio)
LAN	Local Area Network
LEU	Low-Enriched Uranium
LLC	Limited Liability Company
LOPA	Layer-Of-Protection Analysis
Ltd.	Limited (company)
M.Sc.	Master of Science
MAC	Media Access Control
Mbit/s	Megabits per second
MD5	Message Digest 5 (algorithm)
Meterpreter	Meta-interpreter
MMC	MultiMedia Card
NAT	Network Address Translation
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVS	Non-Volatile Storage
ODVA	Open Devicenet Vendor Association
OEM	Original Equipment Manufacturer
OS	Operating System
Oy	*Osakeyhtiö* (Finnish for incorporated company, Inc.)
PC	Personal Computer
PD	Process Data
PDS	Power Drive System
PDS(SR)	Power Drive System suitable for use in Safety-Related applications
PERA	Purdue Enterprise Reference Architecture
PF	PowerFlex
PID	Proportional–Integrative–Derivative (controller)
PL	Performance Level
PLC	Programmable Logic Controller

Plc	Public limited company
PNO	Profibus NutzerOrganisation e. v.
PPO	Parameter/Process Data Object
PROFIBUS	PROcess FIeld BUS
PROFINET	PROcess FIeld NETwork
PTC	Positive Temperature Coefficient
PU	Power Unit
PW	PassWord
RAM	Random Access Memory
RFC	Request For Comments
RJ-	Registered Jack (e.g. RJ-45)
ROM	Read Only Memory
rpm	revolutions per minute
RS-	Recommended Standard (e.g. RS-232)
RSA	Rivest-Shamir-Adleman (algorithm)
RTU	Remote Terminal Unit
S.r.l	*Società a responsabilità limitata* (Italian for LLC, see above)
SBC	Safe Brake Control
SCADA	Supervisory Control And Data Acquisition
SCIM	Squirrel Cage Induction Motor
SET	Social Engineering Toolkit
SFD	Start Frame Delimiter
SI	System Integrator
SIEM	Security Information and Event Management
SIL	Safety Integrity Level
Sin/Cos	Sine/Cosine (signals)
SIS	Safety Instrumented System
SM	Synchronous Motor
SNMP	Simple Network Management Protocol
SLS	Safely-Limited Speed
SP1	Service Pack 1
SRP/CS	Safety-Related Parts of Control Systems
SS1	Safe Stop 1
SSI	Synchronous Serial Interface
SSR	Safe Speed Range
STO	Safe Torque Off
SWU	Separative Work Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
THC	The Hacker's Choice
TTL	Transistor-Transistor Logic
U.S.	United States (of America)
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus

VFD	Variable Frequency Drive
VM	Virtual Machine
VPN	Virtual Private Network
VSI	Voltage Source Inverter
VSD	Variable Speed Drive
WLAN	Wireless Local Area Network
WWW	World Wide Web

1 Introduction

An alternating current (AC) drive is a place where cyberspace meets the physical world. Digital control signals, sent from far reaches of interconnected computer networks, are translated to electric energy by power electronics inside an AC drive. This electric energy is transformed to mechanical energy in electric motors driving heavy machinery. But what happens to the machinery if the control signals are not what they are supposed to be?

The results of the probably most notorious example of cyber sabotage can be read from reports like the one by Albright et al. [2010]: The machinery was physically damaged and had to be replaced, causing disruptions to the production process, not to mention replacement costs. That damaged machinery were hundreds of gas centrifuges, enriching uranium at the Natanz enrichment plant in Iran.

And what caused the Iranian gas centrifuges to fail with devastating consequences? According to Albright et al. [2011], the reason was excessive rotational speed and destructive centrifugal forces with it. The gas centrifuges were not in control of the plant operators anymore, but instead they were attacked by a *weapon of cyberwar* called Stuxnet.

This master's thesis is about securing an industrial AC drive application. The goal is to find a solution to secure the drive application in such a way that damage is not inflicted upon the equipment or people, in case the control system has been compromised. Possible solutions will be presented as guidelines for the design of the AC drive application, potentially including drive features and configuration options.

The initial hypothesis is that any control systems can not be trusted, i.e. assumed secure, and the drive application must be protected by some kind of safety/protection system. It must be possible to prevent physical destruction somehow, at all times.

Due to the vast of amount of different industrial AC drive applications, the scope of this thesis is limited to one specific application: the *decanter centrifuge*, also known as a *solid-bowl, scroll-discharge centrifuge*. The security practices presented for this one application might be applicable to other AC drive applications also.

The decanter centrifuge was chosen as the target application, because it bears similarities with the machinery attacked by Stuxnet, gas centrifuges, being another type of centrifuge. In addition, AC drives for some decanters are known to be equipped with Ethernet-based fieldbuses and safety features, which both are within the scope of this thesis. And finally, the decanter centrifuge is an industrial application only, which also fits into the scope.

Usually, when discussing about AC drives, cybersecurity is not among the top issues on the agenda. AC drives are used in all sorts of applications, ranging from industrial decanter centrifuges to domestic appliances, such as washing machines. Applications are so numerous that it is practically impossible to know them all. The application subject was chosen industrial, because virtually all industrial facilities have one or more AC drives. Thus, the industrial sector is a huge market for AC drives.

The industrial environment examined in this thesis is also limited. Security breaches in the manufacturing process of an AC drive and related equipment are not

taken into consideration. So it will be assumed that every AC drive, programmable logic controller (PLC), and other piece of equipment delivered to the end-user is not compromised, without any (intentionally) malicious code running on it. The production plant and the supply chain will be considered secure in that way. Any possible security breaches are assumed to be happening at the end-user's premises, at the site of the decanter centrifuge.

However, in reality, production plants of component manufacturers can be even more vulnerable to external and internal threats, compared to facilities of end-users. It is also possible that a manufacturer *intentionally* delivers equipment with "backdoors", e.g. for espionage purposes, like some Chinese companies have been accused by the United States (U.S.) congress recently [Rogers and Ruppersberger, 2012, Schmidt et al., 2012].

Furthermore, it will be assumed that the decanter centrifuge is physically secure, i.e. a potential attacker has no physical access to conduct sabotage. Usually that is the case, as decanters are used in industrial facilities with locked doors, burglar alarms, and security guards. Additionally, AC drives are often located in locked electric cabinets. Thus, the only way for a cyber attacker to reach the decanter application and the AC drives is through a medium introduced to the network (e.g. a laptop) or a device connected to the AC drives (e.g. a PLC).

Unlike most of the publications about security of industrial control systems (ICS's), the subject is examined as the AC drive as the central piece of equipment. Usually in other studies, logically upper control systems (e.g. PLC and networks) are considered as the central element, and their security is analyzed. However, modern premium AC drives include many of the functionalities that external PLC equipment have, such as user programmable (firmware) applications with extensive function block sets, and multiple different fieldbus connection possibilities. In some applications and configurations, these services offered by individual AC drives are enough, making any additional PLCs redundant.

The first major, wide-scale incident against ICS's was due to the malware named Stuxnet, which also has received a lot of media coverage. There have been other cyber attacks against industrial facilities in the past, but they have been mainly constrained to single facilities, unlike Stuxnet which spread to many countries (although probably unintentionally) [Falliere et al., 2011, p. 7].

This thesis is not about cyber weapons or cyber warfare in general. Although Stuxnet, which can be categorized as a cyber weapon, is analyzed, it is only done for background research purposes and the main focus is on protecting the decanter centrifuge from whatever cyber threats.

It is a general principle in the field of cybersecurity that to assess vulnerabilities of a system, one must think like *an attacker*. This principle is borne in mind while the components of the decanter centrifuge are inspected later in this thesis. A possible related scenario imagined for that is a terrorist group with substantial resources, wanting to demonstrate their cyberwar abilities by wreaking havoc in some water treatment facility, before targeting a nation's energy supply by disrupting production of an uranium mine. This scenario is totally fictitious without any reference to real life incidents.

The benefit this thesis seeks to bring is to widen the knowledge of cybersecurity issues among the automation industry, see how well AC drives can be secured, and improve their security and safety. Target audience are manufacturers of AC drives, original equipment manufacturers (OEMs), and system integrators (SIs) operating in the machinery and automation industry.

For starters in this thesis, a brief primer about cybersecurity, traditionally known as *computer security* or *computer network security*, is presented in Section 2. After the reader is familiarized with the basic concepts, the Stuxnet case will be dissected in Section 3, to find out how physical destruction was ultimately possible. The results of that thorough study shall be utilized in further analysis with the decanter centrifuge application in Section 4, as the vulnerabilities associated with its different components are examined.

Next, theories of security and safety in industrial applications are described in Section 5, along with the latest guidelines. This section is mostly based on literature review, providing the methods for the goal of this thesis.

As a prologue to the experimental part, the AC drives selected for comparison and the software tools to be used are introduced in Section 6. Included among those is the BackTrack Linux distribution, which shall be the main "toolbox" for assessing security vulnerabilities. BackTrack is widely acclaimed in the computer security industry, and is actively developed and maintained. It includes many open source applications for vulnerability assessment of wireless local area networks (WLANs), operating systems (OS's), and industrial control systems (such as Wireshark, Metasploit, and many more).

Comparison of security related features of different AC drive models is detailed in Section 7. The safety and security features of different AC drives shall be studied, to get a view of those features among different manufacturers. In addition to studying the features, vulnerabilities shall be examined with penetration testing tools. The vulnerability assessment of fieldbus communications shall be limited to those of Ethernet. Ethernet is becoming more and more common interface for drives in industrial environment, and new AC drive models often have it as built-in.

Finally, overall results and guidelines for securing the decanter centrifuge are given in Section 8. That along with Section 7 mostly describes the author's original work and conclusions. Vulnerabilities shall be disclosed to some extent. This thesis ends with the summary in Section 9.

2 Cybersecurity

This section introduces the basic concepts and background information related to the subject of the thesis. It is based on literature review and other publicly available information.

For starters, some selected events from history related to cybersecurity are presented as a brief background on how the security situation has evolved. But first, the related terminology used in this thesis is explained.

2.1 Terminology

Gollmann [2011, p. xvii] writes that computer security industry is "a fashion industry", which profits from well-timed "buzzwords". Evidently, *cyber* and related compounds are current buzzwords, which are used even by the President of the United States [Obama, 2009]. Related terms along with their definitions are presented below.

Cyber is derived from the term "cyberspace" which refers to a network of computers and other electronic devices, usually on a global scale [Andress and Winterfield, 2011, p. 2]. (Originally from *cybernetics*, which in turn was derived from the Greek noun *kybernetes* (steersman), according to Langner [2011a, p. 15].)

Cybersecurity "aims at securing the cyber environment", where *cyber environment* means devices and systems, among others, "that can be connected directly or indirectly to networks." [International Telecommunication Union, 2008, p. 2–7]

Cyberwar (cyber warfare) means acts of war, i.e. use of force against an opponent, happening in cyberspace, i.e. against the computer systems maintained by the opponent [Andress and Winterfield, 2011, p. 2–4]. Stuxnet is a prime example of this [Knapp, 2011, p. 37]. According to F-Secure Corporation [2012a, p. 4]: "It's important to understand that cyber warfare does not necessarily have anything to do with the Internet."

Advanced Persistent Threat (APT, not to be confused with the Advanced Packaging Tool used in Linux) "refers to a class of cyber threat designed to infiltrate a network, [and] remain persistent through evasion and propagation techniques". APT is not an act of sabotage, but of espionage, i.e. information theft. Cyberwar may follow an APT. [Knapp, 2011, p. 43, 45, 313]

Cyber threat means a threat to cybersecurity.

Cyber sabotage can generally, in popular media, mean any kind of cyber attack, including deletion of data [Walker, 2012], but in this thesis *cyber sabotage* specifically means physical damage to concrete equipment/machinery as a result of a cyber attack (also known as a *cyber-physical attack* [Hawrylak et al., 2012, Langner, 2012]).

Next, more traditional terms and concepts related to information security (IS) are described, because it is assumed that the reader is not an expert in IS and is more likely involved in industrial automation engineering. Most of the definitions are from the *Jargon File*, which has been spread around the hacker community since the 1970s and is nowadays maintained by Eric S. Raymond [2004b], the author of the *New Hacker's Dictionary*. Another main source is the online glossary of the Finnish F-Secure Corporation [2011], which has been in the IS business since 1988. The general concepts used throughout this thesis are:

Virus is a malicious computer program which infects (integrates into) files on the host computer during execution, initiated by the user.

Worm is a *self-replicating* computer program which propagates over a network without infecting any files on the hosts [Andress and Winterfield, 2011, F-Secure Corporation, 2012b, Raymond, 2004a].

Trojan (Trojan Horse) is a program which appears benign but silently performs another action without the user's knowledge.

Malware is a combination of the words *malicious* and *software*, the general term encompassing viruses, worms, trojans, etc. [F-Secure Corporation, 2012b].

Payload is "an action, program or code delivered to a system by a malware" [F-Secure Corporation, 2012b].

Rootkit means "a kit for maintaining root" [Raymond, 2004a] (and *root* meaning the (super-) user account with the highest privileges on a system) and "a standalone software component that attempts to hide processes, files, registry data and network connections" typically using a kernel-mode driver [F-Secure Corporation, 2012b].

Information security "means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" [Office of the Law Revision Counsel, 2012, Title 44 § 3542 (b)(1)].

Computer security "deals with the *prevention* and *detection* of *unauthorized* actions by users of a computer system", as defined in the *Computer Security* book by Gollmann [2011].

Basically, information security deals with data encryption, while computer security deals with access control. Cybersecurity is the combination of those two in a networked environment.

2.2 Cyber Threats and Selected Incidents

Some of the history of cybersecurity is presented in this subsection to see how the field has evolved. The starting point for the time in history will be the 1980s.

It is obvious that the IS field is too vast to be extensively presented in this thesis. Thus, only selected, relevant issues are discussed.

2.2.1 Computer Viruses

In the early days of personal computing, viruses propagated by diskettes because there was no common network interface which most of the personal computers (PCs) would be connected to. A virus would infect the diskette and after that, as it was accessed by another computer, the virus would start executing. Then it would reside in the memory until another, clean diskette was put into the computer and the virus would infect it also. As long as the virus was active in the computer's memory, any diskettes accessed by that computer would get infected. The virus would also infect executable files, which could get spread by uploading to a bulletin board system (BBS).

With the Internet era, the spreading of computer viruses has become easier and faster. Most of the personal computers nowadays are connected to the Internet, either constantly by a broadband connection or randomly by a dial-up connection. The virus residing in the memory of an infected computer has access to all of the billions of computers connected to the Internet in the world through a common interface and network stack. So a virus can propagate by itself, without the need for someone actually carrying it around. But for a modern virus to propagate to a computer without an Internet connection, it has to implement a form of the traditional "physical" propagation method. That is what Stuxnet did, as will be described later.

Basically viruses are computer programs designed to "attack" computers. They are one type of cyber threat, traditionally without a specific target. However, more serious threats usually have one very specific target. For example, Stuxnet can be categorized as a "mostly harmless" virus, but taking into account its target and the possible motivation behind the attackers, it can be considered as the worst kind of cyber threat (as will be further explained later). Progressing along the increasing severity axis, another type of cyber threat are hackers, who do targeted attacks, often without leaving a trace of themselves.

2.2.2 Hackers and Crackers—Case GMail

According to their original meanings, a *hacker* and a *cracker* were two different things. Definitions for them are the following:

Hacker is "an expert or enthusiast of any kind" [Raymond, 2004a] but generally used by the popular media to refer to anyone who attacks against computer systems [F-Secure Corporation, 2012b].

Cracker is "one who breaks security on a system" [Raymond, 2004a], contrary to the original meaning of a *hacker*. Nowadays not widely used and generally replaced by the expansion of the meaning of the term *hacker*.

Hacking is the activity a hacker does, e.g. studying a computer system or breaking into one.

The Conscience of a Hacker is a text written by Loyd Blankenship [1986], known by the alias The Mentor in the hacking community during the 1980s. The text

describes a hacker's state-of-mind very vividly. It can provide some insight of the motives of traditional hackers to the automation industry, such as pure curiosity.

In recent years, political and economical motives for hackers have increased. Economical motives are behind "cyber criminals", who seek economical gains with their "cyber crimes". Political motives are behind people who can be identified as "hacktivists". And like in everything else, there are parties which are hard to categorize, such as the now disintegrated group of hackers who called themselves LulzSec. They attacked multiple government agencies, including the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), defense contractors, and corporations, such as Sony, among others [Winter, 2012].

A couple of years ago, an attack against some Gmail accounts belonging to Chinese human rights activists was traced (by Google) to have originated from China. Although this sparked a major suspicion over the Chinese, the result can not be trusted 100% and there is always some kind of possibility for a cover-up. Maybe that is the reason that no direct consequences or charges have been placed against China or Chinese individuals due to those hacking activities. [Drummond, 2010] Their motives were most likely political, possibly supported by a nation state.

A method called *social engineering* has been proven as a highly effective hacking technique. Basically, it is an exploit against *wetware*, i.e. humans (as opposed to *software* and *hardware*). When considering information security, the human element is a major factor. Even the best technical security measures can be futile if a person operates against them, e.g. by using a weak password.

Also, the actions of one person can affect the security of another person, as was the case in the recent hack incident which involved social engineering exploit against the phone support service of Apple Corporation. It led to the user account of one person being handed over to the "hacker" by the support personnel. [Honan, 2012] After being disclosed publicly, the incident led to companies changing their procedures regarding password resets [Baldwin, 2012, Olivarez-Giles, 2012].

Similarly to other exploits, there are tools for social engineering, most notably *Social Engineering Toolkit (SET)*, developed by David Kennedy of TrustedSec, LLC [2012], who used to work for the U.S. National Security Agency (NSA). SET allows utilization of several *attack vectors* through email, web, and portable media, all requiring user interaction to be successful.

2.2.3 Insider Threat—Case Maroochy Shire

An attack is also possible by an *insider*, which was the case in the cyber attack against the Australian Maroochy Shire area sewerage system in 2000. According to the report published by the U.S. National Institute of Standards and Technology (NIST) [Abrams and Weiss, 2008], a disgruntled former employee of a contractor for the Maroochy Shire council, who had previously installed radio-controlled supervisory control and data acquisition (SCADA) equipment for pumping stations, operated the pumps remotely leading to overflow of 800,000 liters of raw sewage spilling to local parks, rivers, and hotel grounds. The environmental impacts were considerable, including deaths of sea animals and unbearable stench. The perpe-

trator was finally caught after at least 46 unauthorized intrusions to the sewerage control systems between February and April in 2000. According to the NIST report, the SCADA systems on the 142 affected sewage pumping stations did not have "cyber security defenses", which possibly would have helped to mitigate the effects of the attack and track down the intruder sooner. [Abrams and Weiss, 2008, Smith, 2001]

Regarding the Maroochy Shire case, it is important to note that the attacker never was directly employed by the organization he attacked. Instead, the attacker used to work for a contractor, and had the knowledge and the tools to conduct a successful attack. Due to this, the report by Abrams and Weiss [2008, p. 8] names the attacker as "the ultimate insider".

2.2.4 Advanced Persistent Threat—Case RSA

Nation states are usually behind another type of threat, called the *advanced persistent threat*. As the name implies, it is technologically advanced over traditional computer viruses, and utilize that to infiltrate, gather information, and stay hidden.

APTs have emerged during the last decade. They have been used in multiple successful cyber attacks. One of those was the stealing of information related to the RSA SecurID two-factor authentication system [Coviello, 2012], essentially compromising the access control system used by many major companies and organizations worldwide. Discovered by Mr. Timo Hirvonen, a researcher with F-Secure, the RSA compromise started with social engineering using a simple "phishing" email containing only 13 words asking to open the `.xls` (Microsoft Excel) file attachment [Goodin, 2011].

One of the *advanced* methods used by APTs is exploiting public-key infrastructure to disguise as a "legitimate program". Usually, a *digital certificate*, issued by a certificate authority (CA), is used to verify the legitimacy of a computer program or an encrypted connection, for example. However, CAs can be compromised. Also, certificates issued to a manufacturer can be stolen and used to disguise malicious applications as legit. [Fisher, 2012a,b] That was done with Stuxnet analyzed in detail in the next section.

3 Case Stuxnet

For years, industrial control systems were assumed to be safe from hackers and other cyber threats. That changed with Stuxnet. It was like the 9/11 for ICS security.

This section focuses on analyzing the Stuxnet malware and its impact on the variable frequency drive (VFD), the AC drive, to gain knowledge of the APT and cyberwar attack methods, and the centrifuge application weaknesses and vulnerabilities. Because, to be able to prepare for something, one needs to know what to prepare for.

3.1 Overview

This subsection presents an overview of the Stuxnet case, mainly focusing on the features and mechanics of the Stuxnet malware. For starters, the source material is introduced.

3.1.1 Source Material

The main source for mechanics of Stuxnet is the public report titled *W32.Stuxnet Dossier* by Falliere et al. [2011] of Symantec Corporation. Most articles and publications about Stuxnet cite the report. That is why it is used as the main source of information on the details of Stuxnet in this thesis also.

Symantec Corporation [2012b] has been in the software business since 1982. Its security products for home and office environments are well-known, and the company has a good reputation among the security industry.

Regarding the effect of Stuxnet to the physical machinery, several reports publicly released by the Institute for Science and International Security (ISIS) are the main source material. The most essential reports are authored by Albright et al. [2010, 2011].

The Institute for Science and International Security [2011] describes itself as a "non-profit, non-partisan institution" focused on nuclear weapons and related issues, founded in 1993 and located in Washington D.C. One of its funders is the U.S. Department of Energy. It is headed by physicist, M.Sc. David Albright, who formerly worked for International Atomic Energy Agency (IAEA) as a nuclear inspector in Iraq [Institute for Science and International Security, 2010]. The reports published by ISIS are cited by news agencies and other organizations all over the world. They are very extensive and rich in details. That is why they are trusted to provide accurate and reliable information about the Iranian gas centrifuge operations also for this thesis.

3.1.2 Threat Classification

By the definition of an advanced persistent threat, Stuxnet is not an APT, but a weapon of cyber war instead. Falliere et al. [2011, p. 1] describe Stuxnet as a "complex threat" and also "a large, complex piece of malware with many different components and functionalities." Knapp [2011, p. 37] used the term *worm* and the

phrase "the new weapon of cyber war", but also similarly to Symantec "complex and intelligent collection of malware". Also Langner [2011b] describes Stuxnet as "the first cyberwarfare weapon ever".

By definition, Stuxnet can be called a *worm*, because it is able to automatically propagate in a network without user intervention. It is *also* able to propagate from *portable media*, such as an universal serial bus (USB) flash storage, but naturally it requires that the portable media is inserted into a Windows computer. On the other hand, the "worm functionality" was just one part of Stuxnet, and similarly to *a virus* it infected files on Windows computers. [Falliere et al., 2011, p. 25–29]

Since Stuxnet, new, similar kind of computer viruses or APTs have been found in the wild, namely Duqu, and the more recent "sKyWIper" (also known as Flame or W32.Flamer [Symantec Corporation, 2012c]). According to the initial analysis and reports, they are believed to be of the same origin as Stuxnet. Duqu is very similar to Stuxnet, and does not introduce any new ground-breaking technologies. On the other hand, sKyWIper seems to be even more advanced than Stuxnet in its malicious techniques, including spreading via fake update through Windows Update mechanism using spoofed Microsoft certificates, created with a *supercomputer* by message digest 5 (MD5) hash collision. But most importantly from this thesis's point of view, neither of them are known to target PLCs or AC drives. In contrast to Stuxnet which was a deliberate sabotage weapon, Duqu and sKyWIper are used for espionage and information gathering. That is why they are not examined further in this thesis, and Stuxnet is the main research subject for background information about the worst kind of threat for an industrial AC drive application. [F-Secure Corporation, 2012a, sKyWIper Analysis Team, 2012, Symantec Corporation, 2011] Next, the discovery of Stuxnet is explained.

3.1.3 Discovery

The Belarusian anti-virus vendor VirusBlokAda was first contacted by their Iranian customer about unexpected computer reboots in June 2010 (the year 1389 in the Iranian solar Hejrī calendar [Abdollahy, 1990]). VirusBlokAda started investigating the issue with their customer and concluded that the computers at the customer's site were infected by malware. They forwarded the case to Microsoft which started working on the issue to patch a *zero-day vulnerability* in Windows exploited by the malware, and named the malware *Stuxnet*, as a combination of some of the file names (`.stub` and `MrxNet.sys`) found inside the malware's code. [Kaspersky, 2011, Marrs, 2010, Zetter, 2011]

Consequently, the details of Stuxnet were published and it gained a lot of interest from the cybersecurity community and also from the general press, as it was reported to be a ground-breaking computer "virus" [DFA Media Ltd, 2010]. Many computer security experts started analyzing the code, and general knowledge of Stuxnet increased as reports were published. The most thorough public report of Stuxnet was made by Falliere et al. [2011] of the Symantec Corporation.

The Iranians have never announced any official press releases nor disclosed any details concerning the incident [Kaspersky, 2011]. Although some short statements

have been reported [Al Jazeera, 2010, Keizer, 2010], including one in November, 2010, at a press conference where the President of the Islamic Republic of Iran, Mahmoud Ahmadinejad, admitted problems with "centrifuges with the software they had installed in electronic parts." [Hafezi, 2010] So everything known about Stuxnet today is thanks to the work and reports by third-party security experts.

The earliest sample of Stuxnet is from June 2009 (according to the compile time). So it was able to stay hidden for at least a year before it was revealed. Without the rebooting problem Stuxnet might have never been found.

Stuxnet was configured to stop spreading and operating after June 24, 2012. So as of this writing, Stuxnet should pose no serious threat in its original form anymore. [Falliere et al., 2011]

3.1.4 Features

Stuxnet targeted German Siemens PLCs with 6ES7-315-2 (series 300) and 6ES7-417 central processing units (CPUs), and Finnish Vacon NX and Iranian Fararo Paya KFC750V3 AC drives connected through Process Field Bus (PROFIBUS) communications processor modules CP 342-5 (by Siemens). The total amount of AC drives from any of the two manufacturers (Vacon or Fararo Paya) must be at least 33, otherwise the (Siemens) PLC will not be infected. Also, exactly the device models mentioned previously must be found. [Falliere et al., 2011, p. 36–49]

A speculative scenario representing progression of Stuxnet is presented in Figure 1. The exact details are unknown, but the diverse propagation abilities of Stuxnet allowed it to update itself from a command and control (C&C) server over the Internet, cross air-gaps on portable media, and spread within a local area net-

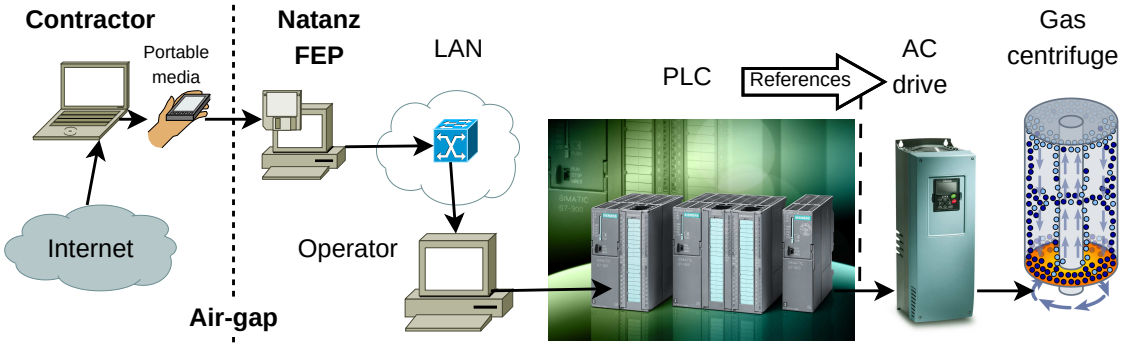


Figure 1: Illustration of progression of Stuxnet from an outside contractor, across the "air-gap" into the production process at the Natanz fuel enrichment plant (FEP). The scenario presented here is speculative. Stuxnet had the ability to spread within a LAN to reach a computer connected to a Siemens PLC [Falliere et al., 2011, p. 25–28]. In the logical chain of interconnected devices, software modifications by Stuxnet stopped after the PLC, and from there on modified control references were used to alter the behavior of AC drives. (Press picture of Simatic S7-300 PLCs courtesy of Siemens AG [2011d]. Photo of a Vacon NXS AC drive courtesy of Vacon Group [2010]. Illustration of a Zippe-type gas centrifuge courtesy of Wikimedia Commons [2006]. Other icons courtesy of Cisco Systems, Inc. [2012].)

work (LAN) [Falliere et al., 2011]. In addition, several state-of-the-art malicious techniques against the Microsoft Windows operating system were used, including

- using four zero-day exploits for propagation and injection through privilege escalation
- digitally signed certificates, which were valid at the time but have been revoked since (one of them issued by Realtek Semiconductor Corporation and the second one by JMicron Technology Corporation, both located near each other in Hsinchu Science Park in Taiwan [Reid, 2012, slide 11])
- Windows rootkit through a digitally signed driver (seemingly legitimate) which hides (filters) files used by Stuxnet from directory listings
- detecting and evading several widely-used antivirus software suites from major vendors, including McAfee, F-Secure, Symantec, etc.
- automatic update mechanism even *without* a network connection. [Falliere et al., 2011]

What really made Stuxnet revolutionary were the several techniques it utilized to attack industrial equipment, like never publicly seen before, including

- first ever PLC rootkit via intercepting communication between the PLC and the Siemens STEP 7 software used to program the PLC, and hiding malicious code from the operator view
- presenting modified information to monitors to hide its actions
- disabling protection functions of AC drives (running centrifuges)
- adjusting control references with intention to physically damage the equipment. [Falliere et al., 2011]

Among the many network propagation methods used by Stuxnet, one was especially specific to ICS: infecting remote computers running the Siemens SCADA software called *SIMATIC WinCC* using a password which was released to the public years earlier. Even though it was in the public, Siemens recommended *against* changing the default password as that would cause other problems. The vulnerability was fixed with the Siemens advisory released on July 23, 2012, *two years* after the discovery of Stuxnet. [Falliere et al., 2011, McMillan, 2010, Siemens AG, 2012e]

Stuxnet replaced a dynamic link library (DLL) file responsible for handling communication between the Siemens STEP 7 programming software and the PLC. This allowed it to read, write, and modify PLC code "blocks". The way the blocks were modified depended on the CPU model of the target PLC and the devices connected to it. [Falliere et al., 2011, p. 36–38] Those requirements are listed in Table 1.

Table 1: The requirements for the PLC CPU and connected AC drives for each infection sequence of Stuxnet. Sequence C is incomplete and disabled. [Falliere et al., 2011, p. 7, 38–39, 45–46]

Infection	CPU	AC drives
Sequence A	6ES7-315-2	Vacon NX
Sequence B	6ES7-315-2	Fararo Paya KFC750V3
Sequence C	6ES7-417	Unknown

3.1.5 Programmable Logic Controller Infection

To "infect" the PLC, Stuxnet modifies the existing blocks and writes new ones according to the infection sequence matching the target devices (Table 1). The original `DP_RECV` block, responsible for receiving PROFIBUS frames, is copied to function block 1869 (FB1869), and then replaced by Stuxnet for post-processing of PROFIBUS data. PLC program entry-points, organization blocks 1 and 35 (OB1 and OB35), are modified by inserting code to the beginning of the blocks ("prepending"), thus ensuring the execution of Stuxnet's code on the PLC. [Falliere et al., 2011, p. 39]

The actual operation of a PLC infected by Stuxnet depends on the infection sequence (Table 1). Although the most complex part of the PLC codes, sequence C is incomplete and disabled in the three different variants of Stuxnet discovered among the 3,280 unique samples received by Symantec. Consequently, in reality Stuxnet infects only Siemens S7-315-2 PLCs by sequences A and B, which differ from each other practically only in the number and format of PROFIBUS frames sent to AC drives. [Falliere et al., 2011] (Figure 1 includes a photo of S7-300 family CPUs for reference.)

Executing inside the PLC, sequences A and B include a complex state machine, with a total of six states, numbered 0–5. Actual sabotage commences in states 3 and 4 as two network bursts of (PROFIBUS) frames carrying parameter values to AC drives. The purpose is to change output frequency of AC drives from the normal 1,064 Hz to 1,410 Hz and 2 Hz, i.e. speed up and slow down the motor. Essentially, that is done by setting the parameter for the maximum frequency to a new value, changing the speed response for the reference value of 100%. [Falliere et al., 2011, p. 41–44]

The AC drives were only following the reference from the master controller, the PLC. Vacon Plc [2010b], the manufacturer of one of the AC drives targeted by Stuxnet, even issued a press statement in which they said that the equipment manufactured by them was not infected and was working correctly. (They also wanted to make clear that they did not sell their equipment "to Iran against the embargo".)

3.1.6 The Target and Damage Inflicted

Stuxnet was a targeted attack against the Natanz fuel enrichment plant (FEP) in Iran. According to Albright et al. [2011, p. 6], "the strongest evidence that Stuxnet is aimed at Natanz" is the part of code of Stuxnet which targets Siemens S7-417 PLCs, dubbed *sequence C* by Falliere et al. [2011]. It includes arrays "identical to an IR-1 centrifuge cascade" at Natanz. (This was found out by the German security expert Ralph Langner [2011a].)

The amount of damage caused by Stuxnet in numbers of destroyed gas centrifuges can only be estimated, as Iran has not released any exact numbers. In an interview by Der Spiegel in 2011, Mr. Olli Heinonen, former IAEA Deputy Director General of Safeguards, estimated that Stuxnet "knocked out almost 2,000 centrifuges in Natanz." [Follath, 2011, International Atomic Energy Agency, 2007]

The report by Albright et al. [2010] about the connection between Stuxnet and the 1,000 replaced IR-1 centrifuges concludes that "Stuxnet is a reasonable explanation for the apparent damage". This finding is based on the quarterly IAEA safeguards reports, which reveal the numbers of operating centrifuge cascades. In the report that followed, Albright et al. [2011, p. 3–4] added referring to the aluminum-based IR-1 centrifuges that "the numbers removed were over and above the normal failure rate, which occurs at a rate of 10 percent per year."

3.1.7 Consequences and Creators

The attack performed by Stuxnet could also occur against civilian equipment. (The uranium enrichment plant at Natanz, Iran, is considered a military installation due to it being administered by the Iranian government.) Stuxnet was like the 9/11 for computer and ICS security. After the 9/11, airplane security was highly increased. Now the same thing needs to be done for ICS security. Since Stuxnet, security of industrial control systems has been under intense public scrutiny. And the media is eager to make flashy headlines about the subject.

It has recently been reported by The New York Times, that the U.S. government was behind Stuxnet along with the Israelis. U.S. NSA and Military Intelligence Unit 8200 of Israel Defense Forces [Haglili, 2012] worked together in Operation *Olympic Games*, launched by President George W. Bush in 2006 and further accelerated by President Barack Obama, to delay Iran's nuclear fuel enrichment as an alternative to a traditional military strike. [Sanger, 2012] U.S. officials have not denied these claims to date.

Stuxnet used two modes for maliciously operating the centrifuges: high speed (1410 Hz) and low speed (2 Hz) [Falliere et al., 2011, p. 43]. It is easy to understand how high speed can be fatal to centrifuge machinery. But the case for low speed is not so self-explanatory. To understand the impact of that, the industrial process in which the centrifuges were involved in must be understood. That shall be described in the next subsection.

3.2 Uranium Enrichment Process

The process of enriching uranium is presented in this section, along with the application for weapon-grade, highly-enriched uranium (HEU).

3.2.1 Uranium

Natural uranium contains three isotopes. Only one of them is *fissile*: the U-235. The rest is mainly U-238 with a trace of U-234. Fissile means fission (split of a nucleus) after absorption of a *zero-energy* neutron. U-235 is *the only* fissile *nuclide* found in the nature. [Lamarsh and Baratta, 2001, p. 77, 119]

A single U-235 fission releases roughly about 200 MeV of energy, which is about *a million times* more energy per kilogram compared to conventional chemical explosives. Most of the energy released is kinetic energy of the fission fragments. [Harris, 2008, Lamarsh and Baratta, 2001] Amount of 9 to 15 kg of highly-enriched uranium with 90% of U-235 is needed to build an implosion-type nuclear weapon, depending on the sophistication of the weapon design. HEU is also called weapon-grade uranium. [Union of Concerned Scientists, 2004]

Natural uranium has only 0.7% of uranium-235 by weight. Thus, it is required to *enrich* the natural uranium to increase the concentration of U-235. [U.S. Nuclear Regulatory Commission, 2011] Enriched uranium can be used to fuel nuclear power plants or as nuclear weapons, depending on the enrichment level. Uranium can be enriched by *isotope separation* with different techniques. One way to separate isotopes is by gas centrifuges. [Wood et al., 2008] Uranium must be in gaseous form for the gas centrifuge process. *Uranium hexafluoride* UF_6 is solid at room temperature, but easily vaporized at an appropriate temperature. [Lamarsh and Baratta, 2001, p. 207–209] UF_6 is produced from *yellowcake*, which is mostly triuranium octoxide U_3O_8 [U.S. Nuclear Regulatory Commission, 2011].

3.2.2 Centrifuge Cascades

A single gas centrifuge can not produce satisfactory enrichment levels. That is why gas centrifuges are "chained" together to formations called *cascades*, with centrifuges connected in series and parallelly. Series connection increases the enrichment level, while parallel connection increases the flow rate of the product (enriched uranium). [Wood et al., 2008] A typical centrifuge cascade consists of 164 gas centrifuges. It can produce 7 grams of low-enriched uranium (LEU) enriched to 3.5% from a feed of 70 grams of natural uranium per hour. [Glaser, 2008, p. 14]

According to the report of U.S. Director of National Intelligence [2012], Iran had produced about 4,900 kg of low-enriched UF_6 at Natanz by November 2010. It has been indicated that Iran is running out of its imported stockpile of yellowcake.

Regarding the production at the Natanz FEP, Albright et al. [2011, p. 10] concludes as follows: "Stuxnet did not lower the production of LEU during 2010. LEU quantities could have certainly been greater, and Stuxnet could be an important part of the reason why they did not increase significantly." The impact of Stuxnet to the production was caused by the combination of destroyed centrifuges, and the

decreased separation performance in those centrifuges which survived overspeeds. Next, the gas centrifuge is presented in detail.

3.3 Gas Centrifuge

As the link between Stuxnet and the Natanz FEP has been established by the ISIS reports (described in Section 3.1.6), this subsection concentrates on the target equipment. That is the gas centrifuge installation in the nuclear facility located about 30 km northwest from Natanz city towards Kashan city, in Isfahan province in Iran [GlobalSecurity.org, 2011].

An example of a centrifuge application from the daily life is the spin cycle of a washing machine: Water with the heavier particles is separated from the clothes with the lighter particles. [Broad, 2004]

The role of a gas centrifuge in the uranium enrichment process is to separate the fissile isotope ^{235}U from the slightly heavier isotope ^{238}U in gaseous form. That is called isotope separation. [Lamarsh and Baratta, 2001, p. 201–210]

3.3.1 Operating Principle

The operation principle of a centrifuge is based on centrifugal acceleration

$$a = \frac{v^2}{r} \tag{1}$$

where v is the radial speed and r is the radius. The direction of centrifugal acceleration is directly away from the center point of rotation. However, usually a *counter-current flow* inside the rotor of the gas centrifuge, which carries the lighter isotopes (U-235) to the top and the heavier (U-238) to the bottom of the rotor, results in an *axial separation factor* much larger than the *radial* separation factor [Wood et al., 2008].

The performance of a gas centrifuge is described by the theoretical maximum *separative work unit* (SWU, expressed here with a symbol better suited for electrical engineering conventions used in this thesis)

$$\Delta W(max) = \frac{\pi}{2} l \rho D \left(\frac{\Delta M v_a^2}{2RT} \right)^2 \tag{2}$$

where l is the length of the rotor of the centrifuge, ρ is the density, D is the diffusion coefficient, ΔM is the difference in molecular weights of two species (U-235 and U-238), v_a is the peripheral speed of the rotor (inner surface), R is the universal gas constant, and T is the temperature of the gas. It shows that the performance is highly dependent on the speed and the length of the rotor. The faster and taller the rotor is, the better the separation performance. [Kemp, 2009, Wood et al., 2008]

3.3.2 Construction of the Zippe-Type Gas Centrifuge

Stuxnet targeted a system similar to the IR-1 centrifuge cascade at the Natanz FEP. The IR-1 is the same as the Pakistani P1 centrifuge, which is relatively old

equipment. During the 1970s, Pakistani engineer A. Q. Khan acquired the design for the P1 from the Dutch gas centrifuge program. Consequently, the IR-1 is a *gas centrifuge*. And more specifically, it is a *Zippe-type* gas centrifuge, based on the work of Austrian scientist Gernot Zippe. [Albright and Walrond, 2010, 2011, Albright et al., 2010, 2011, Kemp, 2009, Khan, 2005, Wood et al., 2008]

The Zippe-type centrifuge (Figure 2) is an advancement over the older *Beams-type* centrifuge, with pivot-magnetic bearing combination to reduce friction. The

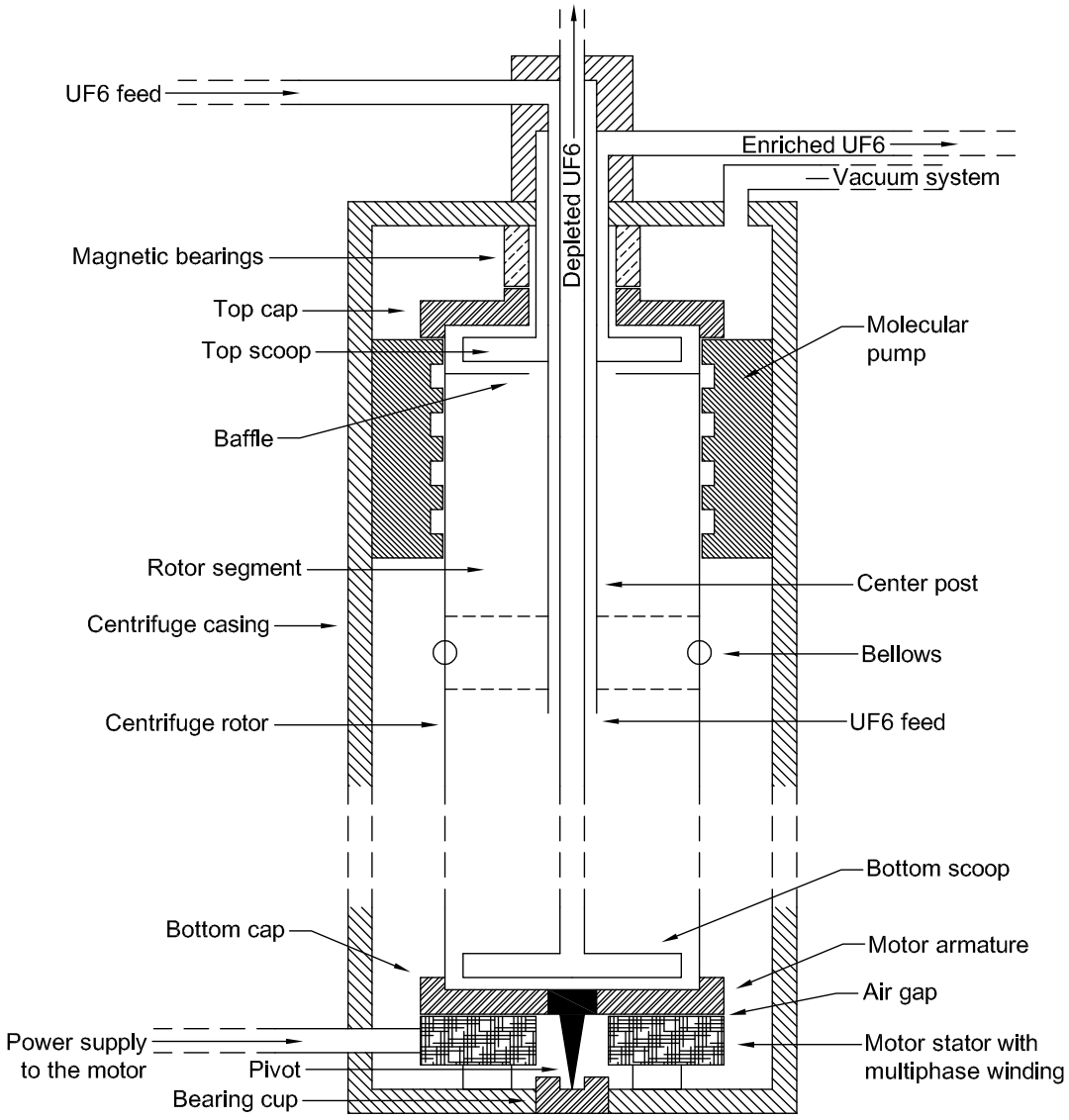


Figure 2: Illustrative representation of an IR-1 Zippe-type gas centrifuge (not in scale). The lengths of the one rotor segment completely visible and the molecular pump have been reduced for illustrative purposes. The rest of the rotor segments along with the bellows have been omitted. The centrifuge rotor is rotating along with the top and bottom caps, the baffle, bellows, and the pivot. Rest of the components are stationary. (The figure is adapted from the figures in the separate works by Lamarsh and Baratta [2001, p. 210], U.S. Department of Energy [1998, p. 3.4–3.9], and Wood et al. [2008, p. 41].)

rotor of the Zippe-type centrifuge rests on a needle-like bearing, a rotating pivot in a bearing cup. It is the only physical contact point of the rotor. The top end of the rotor is hold in place by a *magnetic* bearing, which centers and dampens the vertical motion of the rotor. [Broad, 2004, U.S. Department of Energy, 1998, Wood et al., 2008]

A molecular pump is used to constrain UF_6, leaked from the top (magnetic) bearing, in the upper part inside the outer casing of a gas centrifuge. The outer casing holds vacuum in which the rotor is spinning. [Albright and Hibbs, 1992, Bukharin, 2004]

The aluminum rotor of a Zippe-type centrifuge typically has a diameter of 50–100 mm, a length of 50 cm, and a wall thickness less than one millimeter. The so called *supercritical* centrifuge has a total length of more than 50 cm, but consists of rotor segments each about 50 cm in length, with flexible joints called *bellows* between the segments. A supercritical centrifuge means that it is operating above its lowest natural bending frequency, otherwise it is called *subcritical*. [Institute for Science and International Security, 2002, Wood et al., 2008]

According to an interview of an Iranian official in 2006, the rotor length of an IR-1 centrifuge is 180 cm and the diameter is 10.5 cm, with peripheral velocity of 350 m/s [Glaser, 2008, p. 8]. That corresponds to about 63,662 revolutions per minute (rpm)!

3.3.3 Hysteresis Motor

The enrichment process is assisted by the heat generated by the electric motor at the bottom of the centrifuge rotor [Urenco Limited, 2012]. The main components of the motor are depicted in Figure 3.

The gas centrifuge rotor is rotated by an *axial (flux) hysteresis motor*. The structure of it (Figure 3) is similar to an induction motor, except that the *rotor*, or the *armature*, is constructed of stampings of hardened magnet steel (cobalt-steel)

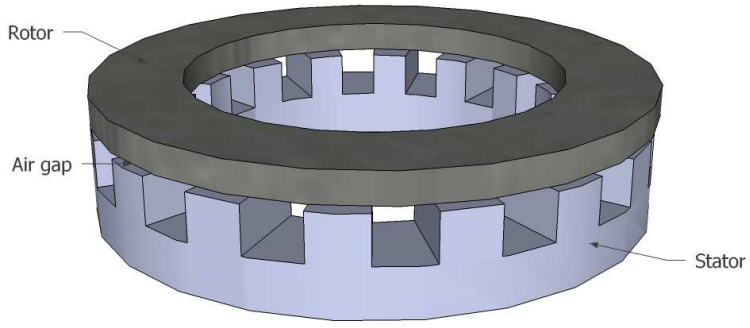


Figure 3: Structure of an axial flux hysteresis motor used in gas centrifuges, without the stator windings and the rotor ring holder (not in scale). The stator (bottom) has a circular iron core with winding slots, similarly to an induction machine. The rotor (top) is purely a ring of permanent magnet material without any windings. (Adapted from the figures by Modarres et al. [2010, p. 323] and Parviainen [2005, p. 17].)

with high magnetic retentivity, and smooth, laminated surfaces. The stator of a hysteresis motor is similar to that of an induction motor, comprised of a circular laminated iron core with multiphase winding. Unlike the induction motor, hysteresis motor is a *synchronous motor* (SM). The magnetic hysteresis is beneficially utilized in this motor, as the power losses caused by it increase the torque. Because of the simple construction of the rotor, the hysteresis motor is reliable and requires little maintenance. Other benefits include noiseless operation and practically constant torque from standstill up to synchronous speed. A gas centrifuge can run for more than 10 years without maintenance, with the motor armature plate (also known as *a drive disc*) attached to the bottom end cap of the centrifuge (Figure 2). [Albright and Hibbs, 1992, Beaty and Kirtley, 1998, Gottlieb, 1997, Institute for Science and International Security, 2003, Modarres et al., 2010, Niasar and Moghbelli, 2012, U.S. Department of Energy, 1998, 2004, Waters, 2003]

The requirements for the AC drive (or the *frequency changer*, as called by International Atomic Energy Agency [2001]) driving the hysteresis motor include a multiphase output of 600–2000 Hz and 40 W or greater, and frequency control accuracy less than 0.1% [U.S. Department of Energy, 2004]. The NX drives by Vacon Plc [2010a, 2012] fulfill these requirements with the high-speed application (firmware ASFIFF12), which has a maximum frequency of 7,200 Hz

According to the application note about high speed applications by Vacon Plc [2007], rotational speed limits and mounting problems of speed feedback devices often inhibit their usage in high speed applications (over 320 Hz). That is why open loop control is required with gas centrifuges.

3.4 Factors Ultimately Contributing to the Physical Destruction

This subsection attempts to explain how Stuxnet ultimately was able to wreak havoc. There are multiple points related to that as discussed in the following subsections.

3.4.1 AC Drive Protection Functions Disabled

According to the report by Falliere et al. [2011, p. 59–67], parameters of the AC drives were altered in such way that all supervisory and limitation functions were disabled. Stuxnet did it through the fieldbus (PROFIBUS). Among the supervisory functions that were set to 0 included (for Vacon NX drives) limits for output frequency, reference, and temperature, motor thermal protection, input and output phase supervisions, earth fault protection, stall protection, overvoltage controller, and underload protection, resulting in most or all built-in protection functions of the drive being disabled. In addition, the current limit was set to 440 A, an unreasonably high value.

Interestingly, the list of the parameters changed includes motor specific values, which should not be touched under normal conditions, after the initial commissioning of the drive. Admitting inaccuracy with some values, Falliere et al. [2011, p. 59–67] list the following motor specific values set by Stuxnet: the nominal input voltage

U_N=380 V, the nominal frequency f_N=80 Hz, the nominal speed n_N=144 rpm, and the power factor cosφ=0.85.

3.4.2 Normal Controller Execution Halted

Organization block 35 (OB35) of the Siemens SIMATIC S7 PLC series functions as a watchdog, executed cyclically every 100 ms. It can stop the execution of the main entry-point for a PLC program, OB1, under certain conditions.

However, during the sabotage routine of Stuxnet, the execution of the original OB1 and OB35 blocks is halted. This effectively prevents operators from gracefully shutting down the uranium enrichment process, if they manage to detect abnormal operation despite falsified data sent to monitors by Stuxnet. [Falliere et al., 2011, p. 38–39, 49]

3.4.3 Response of Other Safety Systems

Regarding operation of other safety systems, Albright et al. [2011, p. 8] speculates as follows: "Safety systems independent of Stuxnet are unlikely to be effective in preventing damage to the centrifuges." Each of the three UF_6 pipes (for the feed, product, and waste) connected to a gas centrifuge (as shown in Figure 2 on page 17) has a fast acting valve, used to stop the gas flow and isolate a malfunctioning centrifuge.

Also, in case of power loss, the valves are used by the safety system to quickly shut off the feed, and empty the centrifuge cascade to prevent the centrifuges from crashing. A sudden deceleration increases pressure inside the center of a rotor, leading to instability.

3.4.4 Destructive Centrifugal Force

According to Albright et al. [2011, p. 9], the rotor tube of the centrifuge formed into a bottle shape by the force of the high centrifugal acceleration, likely breaking the tube. Although, *some* IR-1 centrifuges might have been saved by vibration sensors, triggered by the speed-up, causing dumping of the uranium hexafluoride within milliseconds.

As a conclusion, a gas centrifuge can be damaged not only by high speed, but also fast deceleration. On the other hand, the separation process requires adequately high speed as the separation performance depends on it. Another type of a centrifuge, which will be discussed for the rest of this thesis, is presented in the next section.

4 Industrial AC Drive Application

This section describes the decanter application comprising AC drives, induction motors, and a decanter centrifuge. The decanter is presented with its distinct components, starting with the actual centrifuge machinery itself. But first, an overview of the hardware environment discussed in this thesis is presented in the next subsection.

4.1 Hardware Environment

Hardware environment related to the decanter centrifuge, as assumed in this thesis, is presented in Figure 4. It includes two AC drives in the common direct current (DC) bus configuration, two induction motors, and the decanter centrifuge (machine). Any other possible devices, such as PLCs in the Ethernet network, are not considered. Also, the Internet may or may not be accessible through the Ethernet.

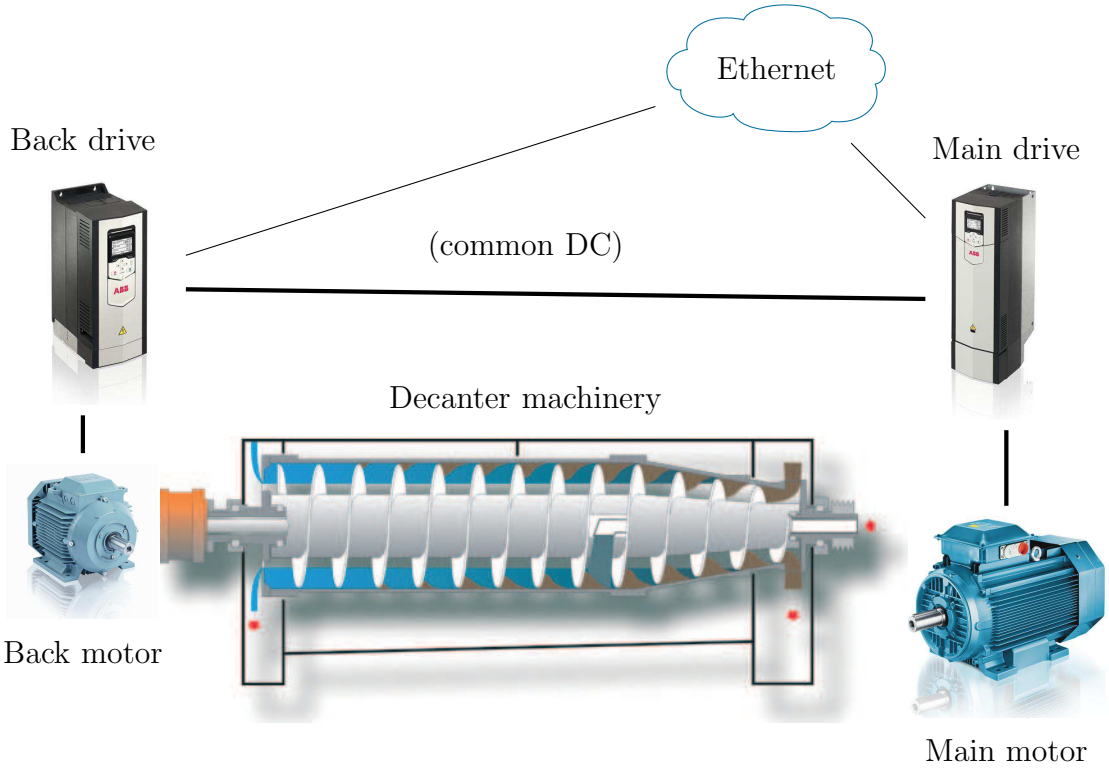


Figure 4: Hardware environment of the decanter application, as assumed in this thesis. It includes the decanter centrifuge machinery with the main motor and the back motor. Both of those induction motors are controlled by AC drives which have a common DC bus. The decanter is connected to an industrial Ethernet network, but other devices in the network are out of the scope of this thesis. (Cross-section of the Alfa Laval decanter model NX 400 courtesy of Alfa Laval Corporate AB [2003] press material. Images of the ACS880-01 drives and the M3AA motors courtesy of ABB [2012c].)

Each of the three distinct components are presented in detail in the following subsections, in the order of the decanter, the induction motor, and the AC drive. (Network, security, and safety issues are discussed later, in Section 5.)

4.2 Decanter Centrifuge

The application of choice for this study is the *decanter*, also known as a decanter centrifuge, a solid bowl scroll centrifuge, and a solid bowl decanter [Poidl and Steiger, 2008]. A decanter is one type of a centrifuge which is used to separate solids from liquids, for example in food, water, and mining industries. Slurry (moist mass) is fed into the decanter bowl, and separated solids and liquids exit. [Yaskawa America, Inc., 2010]

The decanter was chosen as the application for this thesis, because AC drives used in some decanters are equipped with Ethernet connectivity *and* safety features. (The scope of the thesis was limited to Ethernet connectivity, as described in Section 1.) The safety features are required by the decanter application itself, and are not added for security purposes. Also, as a centrifuge, the decanter has similarities with the gas centrifuge application targeted by Stuxnet. Centrifuges are used as separation machines in several industries, including but not limited to the nuclear industry [Comité Européen de Normalisation, 2009, p. 39].

4.2.1 Terminology and Source Material

Some general terms related to decanters as defined in the related European safety standard EN 12547 are presented below.

Centrifuge is a "separation device which has a rotatable chamber in which a mixture of process materials may be subjected to (radial) acceleration".

Decanter is a "continuous working sedimentation centrifuge with an internal screw mechanism for the removal of settled solids from the bowl."

Sedimentation is "separation occurring when the denser or densest part of a mixture in a container settles due to the local gravitational acceleration to the lower part of that container (or outermost zone of a rotating part)." [Comité Européen de Normalisation, 2009, p. 7, 41]

While searching for background material for this thesis, it was discovered that there is very limited amount of detailed information about decanters and even centrifuges in general publicly available. That might be due to the fact that centrifuges (or at least gas centrifuges) are related to regulated nuclear technologies. The main source of information about the details of the decanter application used in this thesis is *Decanter Centrifuge Handbook* by Records and Sutherland [2001]—Alan Records, retired from the Swedish decanter manufacturer Alfa Laval Corporate AB, and Ken Sutherland, an ex-technical manager for the former American centrifuge manufacturer Sharples Corporation, which merged with Alfa Laval in 1988 [Alfa Laval Corporation, 2012]. Alfa Laval is a major decanter supplier world-wide.

4.2.2 Operating Principle

As expressed by Records and Sutherland [2001, p. xiii], the decanter is one particular type of a centrifuge: "the solid-bowl, scroll-discharge centrifuge". Furthermore describing its operation: "The decanter centrifuge is a device for continuously separating particulate solids from a suspending liquid or liquids by sedimentation and decanting." [Records and Sutherland, 2001, p. xiii]

Any sedimenting centrifuge, such as a decanter, relies principally on the centrifugal acceleration, also known as *g-force*, for separating solids from the liquid. The amount of centrifugal acceleration varies inside the bowl, depending on the radius and the depth of the liquid (the *pond depth*). Expressed as a ratio to the gravity, the *g-level*

$$g_c = \frac{\omega^2 r}{g} \tag{3}$$

where ω is the angular velocity of the bowl with radius r, and g is the gravity (≈ 9.81 m/s^2). For example, g-level of 2264 (*times the gravity*) is achieved with a bowl 450 mm in diameter rotating 3000 rpm. [Records and Sutherland, 2001, p. 149–150]

According to Alfa Laval Corporate AB [2008, p. 7]: "The key to good decanter performance lies in the efficient, effective scrolling of the sedimented solids. The design of the screw conveyor is therefore crucial."

The conveyor differential speed (expressed with symbols conforming to electrical engineering conventions used in this thesis)

$$n_d = \frac{n_{bowl} - n_p}{m_{GB}} \tag{4}$$

where n_{bowl} is the speed of the bowl, n_p is the gearbox pinion speed, and m_{GB} is the gearbox ratio, is the speed difference between the bowl and the screw conveyor. With an *epicyclic gearbox*, the differential speed is positive, i.e. the conveyor rotates slower than the bowl. [Records and Sutherland, 2001, p. 150–151]

In conventional dewatering, the differential speed is minimized, to extend the time the cake is dried on the beach. (Also the pond level is minimized to increase the length of the dry beach section.) The required scrolling (conveying) capacity defines the minimum limit for the differential. [Records and Sutherland, 2001, p. 180]

According to Records and Sutherland [2001, p. 151], the conveyor torque

$$T_c = m_{GB} T_p \tag{5}$$

where T_p is the pinion torque, "is a vital measure in the control of modern decanter systems." It results from "moving the separated solids through the bowl, up the beach and out of the decanter." Usually, the conveyor torque is not measured directly, but obtained by Equation (5) with the pinion torque from the braking system instrumentation, such as an AC drive.

With compressible sludges, such as effluents, dryness of the cake (solids) is proportional to the conveyor torque. However, exceeding the practical torque limit of the centrifuge will cause "dirty centrate" (liquids) as a result of overspilling solids. [Records and Sutherland, 2001, p. 185]

The performance of a decanter centrifuge is expressed as the solids recovery (here with an unconventional symbol)

$$O = 100 \left(1 - \frac{Q_l x_l \rho_l}{Q_f x_f \rho_f} \right) \tag{6}$$

where Q_l is the centrate flow rate, x_l is the fraction of solids in the centrate, ρ_l is the centrate density, Q_f is the sludge (process material) feed rate, x_f is the fraction of solids in the feed, and ρ_f is the density of the feed. The higher the O, the better the performance, i.e. the more solids are separated from the input feed. If flocculants (polymers) are used, their dosage also affects performance (the less the better). [Records and Sutherland, 2001, p. 151–153]

4.2.3 Construction

A decanter is "a device" for *decantation* which is a process for the separation of mixtures. The construction and operating principle of a decanter centrifuge is completely different from, for example, a basic household wine decanter, which is used to hold the wine without sediments [Sogg, 2003].

Construction of a decanter centrifuge is depicted in Figure 5. It is similar to the gas centrifuge (previously presented in Figure 2 on page 17): The feed zone is near

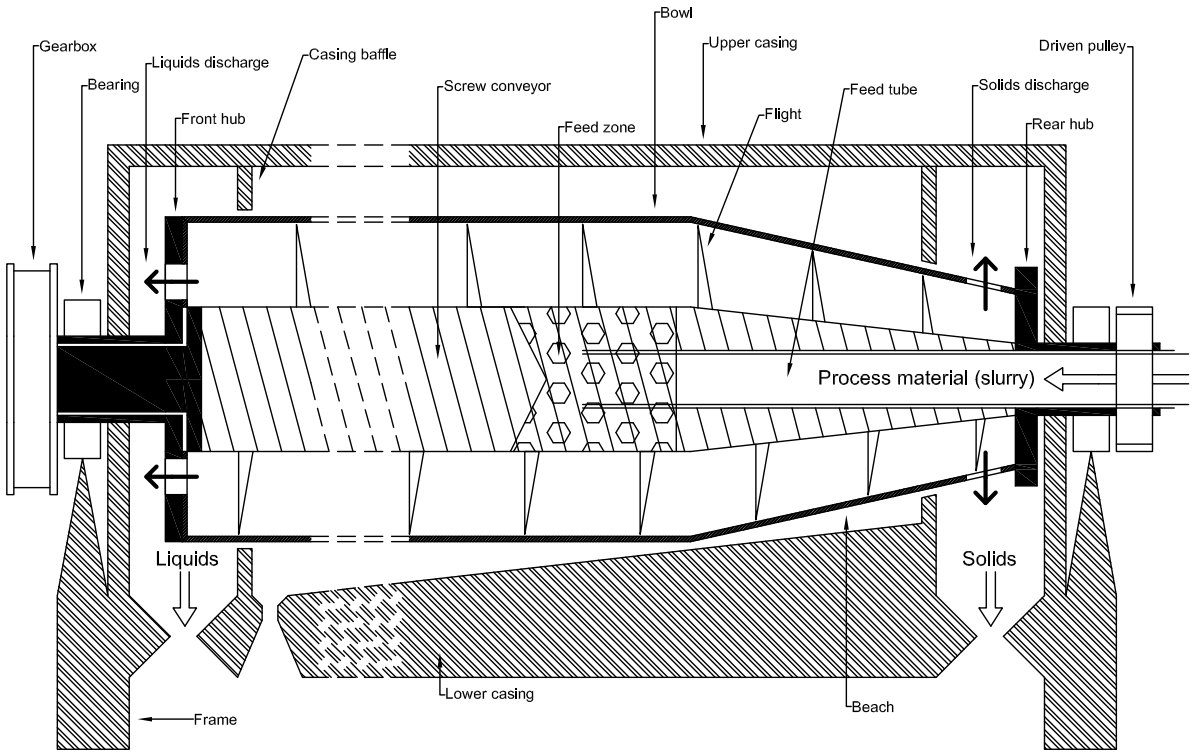


Figure 5: Simplified construction (cross-section) of a decanter centrifuge with counter-current flow. Not in scale. The length has been reduced for illustrative purposes. (The figure is adapted from figures in the separate works by Records and Sutherland [2001, p. 3, 20] and Comité Européen de Normalisation [2009, p. 47].)

the center of the rotor, separated materials are extracted at the rotor ends (comparable to the scoops inside a gas centrifuge), and the length to diameter ratio (L/D) is relatively large. The most notable differences to a gas centrifuge are horizontal alignment and the screw conveyor (the scroll) inside (in the center of Figure 5).

For a decanter according to Records and Sutherland [2001, p. 204–205], larger L/D ratio is better in terms of "overall economy, power consumption and process performance." However, critical speeds (discussed more later) are the limiting factor for the length of a decanter. With design modifications, L/D ratios of over 5 can be achieved.

According to Records and Sutherland [2001, p. 21], the width of the bowl wall depends on the type of material used, "the maximum speed at which the bowl will be rotated, and the maximum weight of process material". The radial clearance between the bowl and the screw conveyor is less than 2 mm, usually 0.5 to 2 mm [Records and Sutherland, 2001, p. 29, 64].

The part of the bowl which helps to raise solids from the pond (the liquid) by the screw conveyor is called the *beach*. According to Records and Sutherland [2001, p. 26]: "A beach angle of 8 to 10 degrees is a common value chosen for many processes."

An actual decanter centrifuge product intended for process industries is presented in Figure 6 as an example. Also the main and the back motors are visible in the photo.

Usually, the main motor of a decanter is an AC motor (with four poles). It rotates the bowl by a set of V-belts. At the opposite end of the bowl, a back drive

Figure 6: The Alfa Laval [2006] decanter model P2-405 for process industries, with maximum dimensions of 457 x 111 x 160 cm (length x width x height) and a weight of 3,800 kg. The bowl, hidden inside, has a diameter of 450 mm and rotates at the maximum speed of 3250 rpm. The inlet is visible at the left side, above the main motor. The back motor is partly visible at the other end of the decanter. Outlets for solids and liquids are hidden in the bottom, between the stands. (Figure courtesy of Alfa Laval Corporate AB [2012] press material.)

system controls the conveyor differential speed through direct connection to the gearbox pinion. [Records and Sutherland, 2001, p. 17, 45]

Decanter designs are variable. There are even vertical decanters, which are more expensive than horizontal designs (depicted in Figures 5 and 6). According to Records and Sutherland [2001, p. 47], vertical decanters are primarily for "high-temperature and/or pressurised operation." Similarly, the Zippe-type gas centrifuge (presented earlier in Section 3.3.2) operates in low pressure, resulting in high vacuum to reduce drag.

4.2.4 Vulnerabilities

It is extremely important not to overload the gearbox above its rated torque, because the *fatigue life* of the gear teeth is proportional to the *ninth* power of the torque. The expected life of the gearbox is *halved* with just 8% increase in torque. [Records and Sutherland, 2001, p. 206]

The bowl of a decanter is subjected to pressure from the material (slurry) inside, and the centrifugal force on the bowl shell material. A maximum speed has to be set for the bowl to ensure safety against failure. [Records and Sutherland, 2001, p. 200–201]

For a decanter, the *first rotor critical speed* means the lowest speed with "significant flexible deformation of the rotor." That is important critical speed and the upper limit for the operating speed. Safe margin is required to ensure that the operating speed stays below the upper limit under normal conditions. [Records and Sutherland, 2001, p. 203] The related terms as defined in the European standard EN 12547 by Comité Européen de Normalisation [2009, p. 9, 41] are presented below.

Critical speed is "rotating frequency of the centrifuge at which resonance of the centrifuge system is excited".

Ultracentrifuge is a "centrifuge having a circumferential speed exceeding 300 m/s." [Comité Européen de Normalisation, 2009, p. 9, 41]

Consequently, the Zippe-type gas centrifuge is an ultracentrifuge, but the decanter is not. For example, the circumferential speed of the decanter in Figure 6 is about 76 m/s. However, decanters have higher inertias.

Records and Sutherland [2001, p. 200] present a very illustrative example of the huge amount of energy in a rotating (running) decanter: The rotational energy of 3.55 MJ of a *medium-sized* decanter, rotating an inertia of 50 kgm^2 at 3600 rpm, "corresponds to the kinetic energy of a vehicle weighing 9.2 tons travelling at 100 km/h." There is major damage potential if that amount of energy gets unleashed uncontrolledly. The safety standard related to this issue is presented later (in Section 5.4.4 on page 54).

Records and Sutherland [2001, p. 204] identify failure of main bearings as "one of the most frequent reasons for breakdown of decanters". Although "a properly designed decanter" avoids "a dangerous situation" in this failure, other parts of the decanter can get damaged. Continuous vibration monitoring systems, with

sensors mounted directly on the bearing housings, are recommended "for critical installations", to detect bearing faults in advance.

According to International Atomic Energy Agency [1980, p. 195]: "The most frequent physical blockage occurs from the collection of sand and other particles in the decanter bottom control valve. This results in failure of the aqueous stream to discharge and raises the aqueous-solvent interface."

4.2.5 Applications

The decanter is mainly an industrial application, as it is pointed out by Records and Sutherland [2001, p. 121] that the "decanter has no place, however, in domestic, institutional or commercial (business) applications, which are covered by separation equipment of quite different kinds." Most of the decanters are sold for water and waste water treatment applications, which constituted 35.1% of market share, according to Records and Sutherland [2001, p. 337].

Similar to the gas centrifuge, the decanter centrifuge is intended for continuous operation and can run unattended for several hours, days, and weeks. In fact, decanters are also used in the production process of uranium yellowcake (which was briefly mentioned in Section 3.2). The production of uranium belongs to the bulk inorganic chemicals industry, which along with other decanter applications related to the minerals industry accounted for 13.4% of the total decanter market value, according to the figures available in 2001. [Alfa Laval Corporate AB, 2007, International Atomic Energy Agency, 1980, Records and Sutherland, 2001]

A high speed, solid bowl decanter is used for *dewatering* in the production of yellowcake [Merkl and Steiger, 2012]. The Alfa Laval decanter model P2 (Figure 6 on page 25) is an example of a decanter for this kind of process.

4.2.6 Decanter Plant and Remote Control

Modern decanters can be integrated with the automation system of a plant, for remote control as an example. Demand for that comes due to many decanter plants operating unattended for many hours daily. It is common to connect the various controllers of the decanter, such as AC drives, to a PLC, which in turn connects to other parts of the plant. [Records and Sutherland, 2001, p. 116–117]

Normally, a fully equipped decanter centrifuge plant has five distinct "modules", which are briefly presented next, in the order following the process flow:

1. The *flocculant system* makes up the polymeric flocculant solution, which is used to increase the size of the particles for more efficient separation.

2. The *process slurry feed system* uses a variable speed pump to feed the slurry to the decanter centrifuge.

3. The *decanter* itself separates solids (the *cake*) and liquids (the *centrate*) from the slurry.

4. The *centrate off-take system* is usually a large pipe leading to a drain or a receiver vessel. Sometimes a pump is used for a pressurized discharge.

5. The *cake discharge system* often uses a belt conveyor to carry the cake into a hopper which is then emptied by a pump. [Records and Sutherland, 2001, p. 215, 317, 365–366]

An integrated master controller for supervision of separate functions of the decanter plant is demanded increasingly. It can be located in a central remote control room for some large plants. Control algorithms of the master controller can be cost-based (economical), such as overall cost or revenue costs minimization. [Records and Sutherland, 2001, p. 328–329] (Negative issues related to remote monitoring and control are discussed later, in Section 5.)

4.2.7 Instrumentation and Controllers

According to Records and Sutherland [2001, p. 321]: "It is particularly necessary to measure the speed of rotation of the decanter bowl and the gearbox pinion shaft. Occasionally a tachometer will be built into the braking device."

There are many controllers involved in the decanter process, for input flow pumps and the main motor, among others. But, according to Records and Sutherland [2001, p. 325–326], the brake controller for the gearbox pinion shaft is the most important one. It can operate in speed mode for the conveyor differential speed, or in torque mode to produce set output torque, which needs to be *reduced* for higher *conveyor* torque because lower differential speed results to increased torque. Indications required from a good brake controller include the bowl speed, the conveyor differential speed, brake or conveyor torque, and high/low alarms for torque and differential (speed). According to Records and Sutherland [2001, p. 326]: "Access is needed to the operating parameters, with an encrypted code to prevent unauthorised tampering." As previously presented in Section 4.1, for the purpose of this thesis it will be assumed that the brake controller will be an AC drive, braking with an induction motor.

4.3 Induction Motor

This subsection describes construction and operating principle of the motor (the electrical machine) powering the application machinery, the decanter centrifuge. Focus is on the induction motor (IM) as it is widely used in the decanter application selected for the scope of this thesis.

The source material regarding the theories for induction motors (and AC drives) are mainly course handouts from Aalto University. The most important papers are titled *Control of Variable-Speed Drives* by Harnefors [2003] and *Sähkömekaniikka ja sähkökäytöt* (Finnish for *Electromechanics and electric drives*) by Luomi and Niemenmaa [2011].

4.3.1 Operating Principle

There are many types of AC motors, i.e. motors designed to run when supplied with AC voltage, usually with three phases. The IM is the most common type of motor used in industry due to robustness, low maintenance requirements, and cheap prices compared to DC motors with equal powers [Luomi and Niemenmaa, 2011, p. 103–104].

Currents in the windings of the rotor of an IM are generated by electromagnetic induction. The induction motor is also known as the *asynchronous machine* (AM), meaning that the rotation of the rotor is not synchronous to the frequency of the stator voltage. [Luomi and Niemenmaa, 2011, p. 103]

The synchronous speed of an electric motor

$$n_s = \frac{\omega}{2\pi p} = \frac{2\pi f}{2\pi p} = \frac{f}{p} \tag{7}$$

where ω is the electric angular velocity of the rotating magnetic field of the stator, f is the frequency of the voltage supplied to the motor (usually 50 or 60 Hz for a line-fed motor), and p is the number of pole pairs. For an AM, rotor currents are not induced during synchronous rotation.

However, the IM is not a SM. Once loaded mechanically, the actual speed of rotation differs from the synchronous speed by the slip

$$s = \frac{n_s - n}{n_s} = \frac{\omega - \omega_m}{\omega} \tag{8}$$

where n is the actual (asynchronous) speed and ω_m is the electrical angular velocity of the rotor. The amount of slip depends on the mechanical loading of the motor, thus also the electrical torque because the induced currents force the rotor to follow the stator flux according to Lenz's law. [Harnefors, 2003, Luomi and Niemenmaa, 2011] (Methods for controlling the speed of an IM are discussed later.)

4.3.2 Construction

There are two types of induction machines, categorized by different rotor constructions: *squirrel cage* and *slip-ring*. Squirrel cage induction motors (SCIMs) are the most common type, with a share of about two thirds of all electric motors. [Luomi and Niemenmaa, 2011, p. 103]

A group of those type of motors is presented in Figure 7a. The physical dimensions of an induction motor, such as the axis height and the total weight, grow along the required output power. Illustrated in Figure 7a, a motor with about twenty times more output power (22 kW with p=2) has doubled axis height (180 mm) and tenfold weight compared (163 kg) to the smallest motor (1.1 kW, 90 mm, and 16 kg) [ABB, 2011a, p. 71–106].

Different numbers of pole pairs affect the way the stator is wound, while the rotor construction is unaffected [Harnefors, 2003, p. 83]. According to Luomi and

(a) (b)

Figure 7: A group of SCIMs (ABB [2011a, p. 71–106] type M3AA made of *aluminum*) with output powers ranging from 1.1 kW at front right to 22 kW at back left (a), and a cutaway view (of ABB type M3BP 315 made of *cast iron*) revealing the inner construction (b). (Photos courtesy of ABB [2012c].)

Niemenmaa [2011, p. 120], most of induction motors have four or six poles, corresponding to pole pair values p of 2 and 3, and synchronous speeds of 1500 and 1000 rpm, respectively.

The inner construction of a SCIM is presented in Figure 7b. On the face of it, the rotor does not look like a traditional "squirrel cage", but the inner construction principle is basically similar—mainly regarding the winding, as the rotor has an iron core. There are conducting aluminum bars in the rotor slots (which are usually skewed to reduce torque pulsations and acoustic noises). The bars are short-circuited by rings at both ends. The rings can also have blades functioning as an internal fan to improve cooling during rotation. [Harnefors, 2003, Luomi and Niemenmaa, 2011]

For an induction motor, which is magnetized from the stator, it is important to have a narrow air-gap between the stator and the rotor. Otherwise more magnetizing current is required in the stator for the desired rotor flux, which in turn causes higher losses in the stator winding and decreases efficiency. According to Harnefors [2003, p. 83]: "IMs rated 100 kW or below have airgaps less than 1 mm wide."

4.3.3 Dimensioning an Induction Motor for a Decanter

To select the main motor for a decanter, Records and Sutherland [2001, p. 197–198] present the following equation for determining the maximum power required at the motor shaft, P_M:

$$P_M \cdot \eta_F \eta_B = P_P + P_{WF} + P_S + P_B \tag{9}$$

where η_F and η_B are efficiencies of couplings between the motor and the bowl, and the rest are separate power components: P_P for accelerating "the process material to the bowl speed at the discharge radius", P_{WF} for windage and friction, P_S for conveying, and P_B for braking. With a regenerative back drive, the braking power

can be omitted. As manufacturers offer motors in standard increments of power, the next larger size should be selected, with as little over-rating as possible for economic reasons.

The torque of the selected main motor needs to be checked to be sufficient to accelerate the bowl smoothly, without the belts slipping. Otherwise the belts will quickly wear out, or even break. Therefore, the run-up (acceleration) time of the motor can not be too short. On the other hand, too long run-up time can result to motor overheat and burn out. As the acceleration time required can be as high as several *minutes*, overload protection using thermistors embedded in the windings of the motor is the only adequate protection method. If tripped, it must be impossible to reset and restart the main motor until it has sufficiently cooled. Consequently, the amount of starts (from zero speed to the full operating speed of the decanter) must be limited within a certain period of time. However, that is typical for normal operation of the decanter which is seldom stopped and restarted. [Records and Sutherland, 2001, p. 44–45, 198–199]

4.3.4 Vulnerabilities in Variable Speed Drive Applications

If an AC drive is coupled to the electric motor, a variable speed (or frequency) drive (VSD/VFD) is formed. A VSD can be controlled. However, the maximum *mechanical* speed of a motor can not be determined from its electrical properties or values. Usually, AC drives need to know only the electrical properties, such as nominal power and frequency, to successfully rotate the axis of the machine with the correct speed (according to the reference). The maximum mechanical speed limit of the motor is determined by the manufacturing process and the materials used. (There are also stricter speed limits due to the application machinery, the decanter centrifuge, as previously discussed in Section 4.2.4.)

For motors, ABB [2011a, p. 10] lists "guideline maximum speed values", which depend on the motor frame size and the number of poles for cast iron motors. Generally, the maximum speed is smaller with a larger pole pair number, as also the corresponding nominal speed is smaller. For the frame sizes presented in Figure 7a, which are in the smaller end of the whole size (power) range offered by the manufacturer, the maximum speeds are the same for 2-pole (p=1) and 4-pole (p=2) models: 6000 rpm for sizes 90–100, and 4500 rpm for sizes 112–200. (It should be noted though, that the motors presented in Figure 7a are made of *aluminum* instead of cast iron, so their speed limits might be different in reality.)

It is common to have positive temperature coefficient (PTC) thermistors in the stator windings, which are used to indicate too high temperature of the motor (usually caused by overloading). That is why many AC drives have inputs for thermistors to protect the motor from overheating damage by cutting off the power supply. Furthermore, for the safety of the application, ABB [2010a, p. 13] recommends using "suitable protective features" of an AC drive, including minimum and maximum speeds, acceleration and deceleration times, maximum current and torque limits, and stall protection. Next, the AC drive is inspected in detail, as it is used more and more especially with the smaller decanters [Records and Sutherland, 2001, p. 45].

4.4 AC Drive

This section describes the AC drive powering the decanter. Electric drives are attractive over other drive systems still used today, including steam engines for aircraft launch assist, hydraulic engines for their extreme power per volume, pneumatic drives for their simplicity and softness, and combustion engines in vehicles [Harnefors, 2003, Veltman et al., 2007].

4.4.1 Terminology and Source Material

First a note about terminology used in this thesis: An AC drive for controlling an electric AC motor is called with many different names. Relevant international standards by International Electrotechnical Commission [1998, 2002] use the term *converter* as a part of an "a.c. power drive system (PDS)". The American Underwriters Laboratories Inc. [2010, p. 9] standard 508C is about safety of "power conversion equipment" which refers to "equipment that supplies power to control a motor".

The term *inverter* is used in the books by Harnefors [2003, p. 59], Records and Sutherland [2001, p. 45], and Beaty and Kirtley [1998, p. 4]. An inverter converts DC to AC, for example a separate inverter product commonly found in the consumer market for cars and boats converts +12 V DC to 230 V AC. (Actually, the inverter is only one part of an AC drive, as will be explained later.)

Major manufacturers, such as ABB, Siemens, Rockwell, and Vacon, seem to prefer the term *AC drive* in their existing sales and marketing materials. According to ABB Ltd [2011], "drive is an electronic device used to regulate the performance of an electric motor". The another popular term "frequency converter" (or changer) has a dual meaning also as a device between two electrical networks with different frequencies, used in bulk energy transmission, which has little to do with controlling a motor. To avoid confusion and use the term which is commonly shared among manufacturers, the term (AC) *drive* is used instead of a *frequency converter* to describe a device for controlling an electric (AC) motor in this thesis, as summarized below.

Drive traditionally means an apparatus which transforms energy in some form into mechanical energy to *drive* a mechanical load, e.g. *electrical drive* [Harnefors, 2003, Luomi, 2010, Niiranen, 2000]. Specifically in electrical context, the term drive (electric drive) usually means an electronic device which controls an electric motor, also known as an AC or DC drive [ABB Ltd, 2011].

AC drive is an electronic device for controlling *an AC motor*.

In addition to the handouts by Harnefors [2003] and Luomi [2010] introduced in Section 4.3, the handout titled *Control of Electric Drives Addenda* by Luomi [2009] is used as the main source material about AC drives and their control methods.

4.4.2 Energy Savings and Applications

According to International Energy Agency (IEA), 42% of all electricity generated in the world is consumed by industry. 70% of that energy goes to electric motors used virtually in all sectors. Over 90% of those motors are not speed-adjusted by AC drives, which offers huge energy saving potential in variable speed applications. Because AC drives save electric energy by controlling the rotational speed of motors efficiently, speeding up and slowing down according to the needs of the process, instead of running at a constant speed all the time. For example, during 2011 all installed drives from ABB saved 310 MWh, which equals to yearly electricity consumption of about 75 million households in European Union (EU), or yearly CO_2 emissions of over 65 million cars. [ABB, 2012b, p. 3–5]

AC drives are used in numerous different applications, not limited to industry only but also in residential, military, and automotive applications, to name a few. More recent AC drive applications (or specifically inverter applications) include hybrid electric vehicles, for example the Toyota Prius car.

4.4.3 Operating Principle

A common misconception about AC drives (especially when addressed as *frequency converters*) is that they are basically like transformers, except that instead of voltage they transform frequency. However, AC drives are control devices, controlling the speed of rotation of AC motors.

For an induction machine, the speed of rotation

$$n = (1 - s)\frac{f}{p} \tag{10}$$

is determined by the stator frequency f, the pole pair value p, and the slip s. Consequently, the speed can be controlled by modifying any of those three quantities. In terms of losses and accuracy, the most beneficial method is to control the stator (supply) frequency by an AC drive (hence also known as a frequency converter). [Luomi and Niemenmaa, 2011, p. 159, 162]

However, frequency control (also known as *scalar control*) is the most basic type of control methods used by AC drives. Vector control allows the stator flux and torque to be independently controlled. Direct torque control (DTC), the motor control method patented by ABB [Heikkilä, 2000] used by some of its premium industrial AC drives such as the ACS880-01 [ABB, 2012d], enables the fastest possible rate of change for torque. Its main principle is to select always the most suitable voltage vector. [Luomi, 2009, Tiitinen and Surandra, 1996]

An induction machine can be used as a motor or a generator, depending on the directions of speed and torque. In a decanter with two AC drives, the back drive (controlling the speed of the gearbox pinion shaft) is generating energy as it is braking (slowing down) for the differential speed of the conveyor, rotating slightly slower than the bowl. The main drive is working as a motor, consuming energy to rotate the bowl. A common DC bus (shared between the drives) configuration allows for utilizing the regenerated power from the back drive. The benefit from that

is smaller total power consumption of the decanter, offering substantial operating cost savings in the long run. [Records and Sutherland, 2001, p. 17, 37, 115-116]

4.4.4 Construction

Generally, an AC drive consists of two distinct main components: the power unit (PU) and the control unit (CU), as depicted in Figure 8. According to Niiranen [2000, p. 50], the most common PU type for AC drives includes the voltage source inverter (VSI). Usually, the VSI type PU consists of three sections or stages: the *rectifier*, the DC *intermediate circuit*, and the *inverter*. The inverter part contains power semiconductors, nowadays commonly insulated gate bipolar transistors (IGBTs), used to generate the required voltage form for the motor. The power flows through the different PU stages according to operation by the CU, as indicated in Figure 8. (A photo of an actual AC drive is presented later, in Figure 10 on page 36)

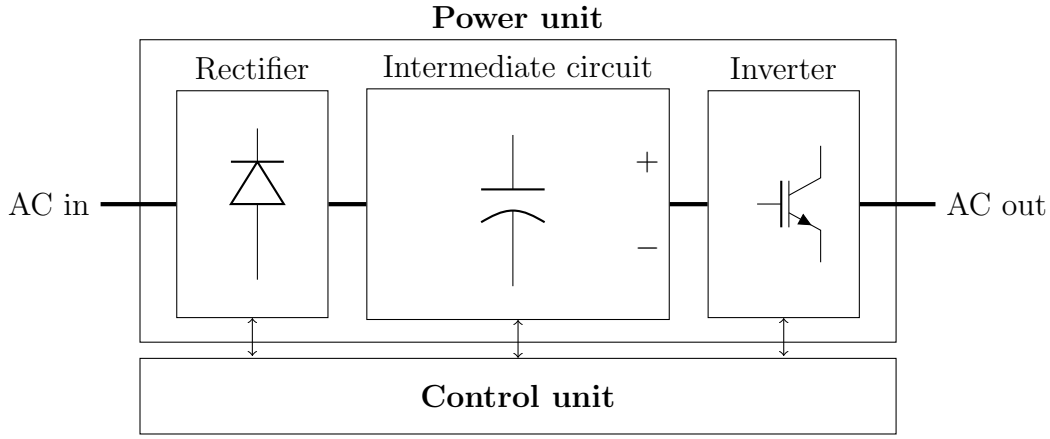


Figure 8: Generalized diagram of different components inside an AC drive with voltage intermediate circuit, from left to right: the rectifier (AC→DC), the DC intermediate circuit (with capacitors for storing energy), and the inverter (DC→AC) with IGBT switches. The control unit monitors and operates the components inside the power unit according to the firmware.

Universally, a three-phase power supply is used in industrial applications. That is beneficial for rectification, as three-phase rectifiers have smaller harmonic components in the DC voltage and supply currents. [Kyyrä, 2009, p. 152]

Considering motor control, the most important electronic components inside an AC drive are the switches in the inverter bridge at the output. The evolution of IGBTs, notably their voltage and current ratings, have made them practical in many AC drive designs.

4.4.5 Performance Challenges in Decanter Applications

According to Yaskawa America, Inc. [2010, p. 1], performance challenges for AC drives in decanter applications include: high torque near zero speed, “a very high-

reflected inertia" with the bowl, torque limitation on the scroll (the screw conveyor), and possibly dynamic or regenerative braking.

Modern motor control methods are efficient for the performance challenges described above. With state-of-the-art control like DTC, the decanter can operate smoothly as the AC drive takes care of the possibly varying process conditions. Upper control systems need only to provide a reference which the drive will fulfill.

4.4.6 Reference Chain, Limits, and Protections

Most AC drives have some kind of basic protection functions to protect the motor from too high current, for example. A typical reference chain is presented in Figure 9. It consists of two controllers for speed and torque, and limiters for their input and output values. This kind of scheme, with the torque control loop inside the outer speed control loop, is called *cascade control*. (For motion control applications, there is a third controller for position located outermost of the cascaded control loops.)

The reference type depends on the active control mode of the AC drive. Usually, in speed control mode, the unit for the reference is hertz (Hz) or revolutions per minute (rpm). Torque control mode commonly uses the reference as a percentage of the nominal torque of the motor (T_N).

As previously briefly mentioned in Section 4.3.4, induction motors have maximum speed limits which are not related to their electrical properties. So, it is possible that the AC drive tries to run the motor at such speed which is dangerous to the motor and the decanter, leading to physical damage. That is why it is common to have configurable maximum (and minimum) speed limits in AC drives. But usually they can be set to any value the user/operator chooses. And it is also possible that, due to a flaw in the AC drive's firmware or some control-loop malfunction or misconfiguration, the motor is run at speeds exceeding the maximum speed limit set in the drive. This can be avoided by using an external safety speed monitoring module which either limits the speed, or stops the motor completely in a safe way.

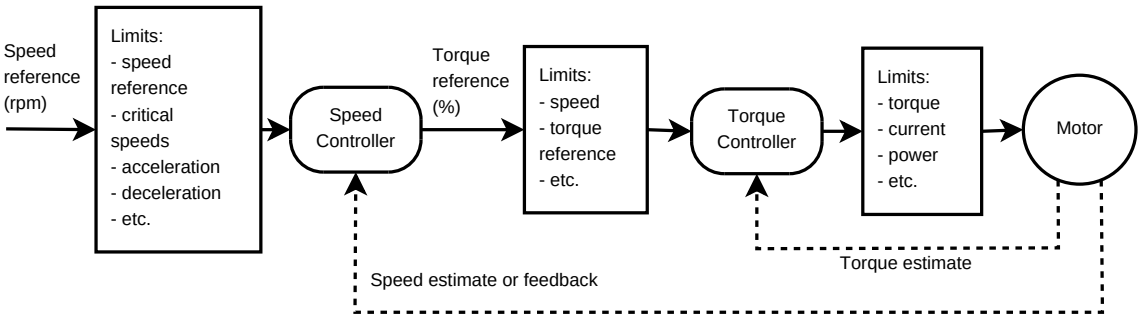


Figure 9: Simplified diagram of the reference chain of a typical AC drive with speed and torque cascade control, where the speed controller supplies the torque reference to the torque controller, based on the speed reference from upper control systems. Limit functions are provided at the inputs and outputs of each controller to protect the motor and other machinery. (Adapted from the figures by Niiranen [2000, p. 68] and ABB Oy [2012c, p. 347–363].)

(This kind of safety functionality is further discussed later.)

Other protection functions required in the decanter application (also commonly in other applications as well) are motor thermal overload protection using a thermistor in the windings (discussed in Section 4.3.4) and acceleration time limitation to prevent slippage of the belts (described in Section 4.3.3). For the back drive, torque limit is important for protection of the gearbox (discussed in Section 4.2.4). However, those protection functions are of little use against cyber sabotage if they can be disabled remotely without authentication.

The limits and other configuration options of AC drives can be changed by software *parameters*, generally accessible through a human-machine interface (HMI) and an optional fieldbus. There can be as many as *thousand* different parameters in a single AC drive. Usually, some parameters can not be changed while the drive is running, but in stopped state there are often no restrictions.

4.4.7 Control Interfaces

Generally, the reference to the drive can be supplied from three different locations: the operating/control panel (hand-held or a *PC-tool*), the basic analog and digital input/output (I/O) signals, and the fieldbus. Usually, only one of those control locations can be active at a time.

The connection environment for operating the drive, as assumed in this thesis, is presented in Figure 10. For this thesis, the most notable control location is the Ethernet based fieldbus, along with the safe torque off (STO) control for functional

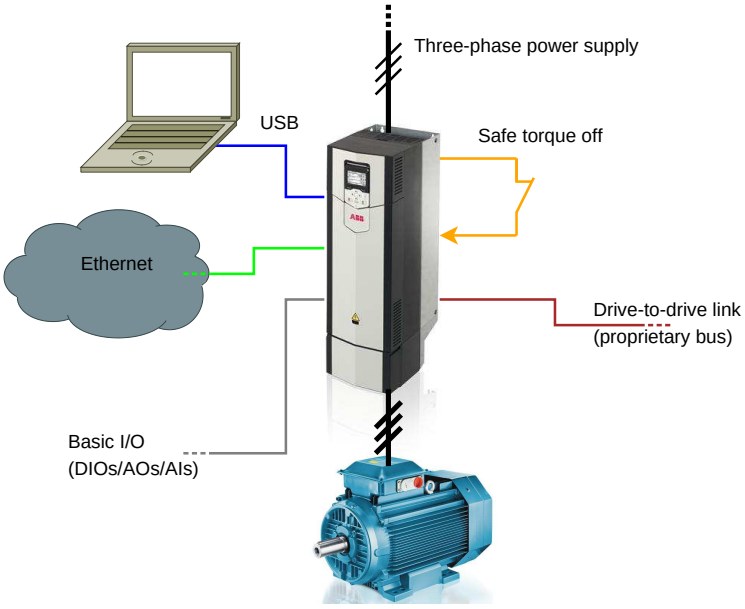


Figure 10: Some connection interfaces to an AC drive: The USB, the Ethernet based fieldbus, the basic digital and analog I/O, the STO for functional safety, and a manufacturer specific proprietary bus (e.g. drive-to-drive link) [ABB Oy, 2012e] (Images of the ACS880-01 drive and the motor courtesy of ABB [2012c]. Network related icons courtesy of Cisco Systems, Inc. [2012].)

safety. Also, the universal serial bus (USB) or other interface for a PC-tool is important, because it allows configuration and modification of the drive operation. In the next section, the control interfaces are discussed thoroughly, because they are the paths (also called *attack vectors*) to commit cyber sabotage against the decanter centrifuge.

5 System Security and Machinery Safety

This section focuses on safety and security aspects of industrial equipment, taking a top to bottom approach starting from the network, and going through the field level to the machine-specific safety. Those subjects are essential for determination of proper methods for protection of the decanter centrifuge against sabotage by a Stuxnet-like cyber threat. The selected, applicable methods are presented and their justification discussed.

5.1 General

This subsection presents general information related to both security and safety subjects discussed in this Section 5. Firstly, the source materials and terminology are presented.

5.1.1 Source Material and Terminology

This Section 5 is mainly based on literature review. The source materials are the following: Regarding network security, the main source is the book *Industrial Network Security* by Knapp [2011]. It is all about information technology (IT) security without going into safety and physical machinery. The security guidelines presented in the book are summarized in Section 5.2.3.

Another main source book is *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet* by Langner [2011a]. Some of his ideas about risk determination are included in Section 5.1.2, while others are scattered throughout the whole Section 5, including some mentions about safety.

Both of the those books are post-Stuxnet, meaning that they have been published after the discovery of Stuxnet in 2010. Both works address Stuxnet somehow, even briefly. Therefore, they are up-to-date on the latest threat posed to industrial control systems, contrary to most pre-Stuxnet books.

Regarding fieldbus security, the main source is *White Paper on Industrial Automation Security in Fieldbus and Field Device Level* by Sundell et al. [2011]. It was published by Vacon Plc, one of the two AC drive manufacturers specifically targeted by Stuxnet (as previously described in Section 3.1.4).

Source material for safety is more scattered, without a single distinct main source. Nevertheless, the book titled *Safety Instrumented Systems: Design, Analysis, and Justification* by Gruhn and Cheddie [2006] deserves to be mentioned as an excellent book on industrial process safety matters, used in this thesis also. Even though published before Stuxnet, the principles described in it stand the test of time.

It is important to distinguish the differences between the terms *security* and *safety*. They are used in this thesis as follows:

Security means “measures taken to guard against espionage or sabotage, crime, attack, or escape”.

Safety means “the condition of being safe from undergoing or causing hurt, injury, or loss”. [Merriam-Webster, Inc., 2012a,b]

Those definitions are shared among the automation and security industries, as described by Byres and Cusimano [2010].

5.1.2 Risk Model

According to International Telecommunication Union [2008, p. 8]: "Security is all about risk management." Many techniques can be used to manage risks, including detection, countermeasures, and a recovery strategy.

This subsection discusses risks mainly to the extent Langner [2011a] presents them in his book. However, diverging from traditional IT security doctrines, risk concept and the terms *confidentiality*, *integrity*, and *availability* are put aside for a new perspective based on the realization that improving security actually means "making fragile systems more robust" [Langner, 2011a, p. x].

According to Langner [2011a, p. 4]: "Security researchers and vendors of security products (who benefit from perceived high threat levels) tend to exaggerate threats, whereas asset owners (who benefit from perceived low threat levels) tend to deny threats. Even where there is evidence of threats and related risks, one may choose simply not to trust the underlying prediction."

Out of the three risk models (insurance, logical, and financial) Langner [2011a, p. 1–7] presents at the beginning of his book, he chooses the financial model as the best one for his approach to improving the security (or *robusting*, as he calls it) of an IACS. In the financial model, risk is seen as *volatility*, which means *variability*. A volatile investment has the potential for bigger profits than a safe investment. However, contrary to the finance sector, in industrial automation volatility is bad, and a system showing volatile behavior is not fully controlled. Improving the controllability of a system should be a major motivator to enhance its security. Langner [2011a, p. 7] points out, that "risk and security are hypothetical", but control of a system is "factual".

Reduction of risk (or volatility) can be achieved by reducing *undesired output variation* of the system. That is the same as gaining more control over the system and being able to predict it more accurately. Reducing *uncontrolled factors*, of which the system is dependent on, results to less of volatility, less of risk. [Langner, 2011a, p. 6]

Following this introduction, Langner [2011a, p. 7] lets go of the term *risk* and substitutes the terms *fragility* for high risk and *robustness* for low risk. And more specifically, for the context of his book, the concepts are limited to "*cyber fragility* and *cyber robustness*." Using those terms, there is less room for arguing that ICS security issues might be only hypothetical.

According to Langner [2011a, p. 175]: "Robustification is not about defense and mitigation. It is not primarily *against* anything." Instead of focusing on external factors, robustification leads towards an inherently better system, with minimal *fragility*.

Robustification procedure involves many steps. One of them includes "surplus strategies" which enhance a system or a process by adding something more it, for example safety and monitoring systems, redundancy, and derating i.e. performance

margins. They are to be implemented after "reduction strategies" which harden a system by removing unnecessary services and restricting user access for example. [Langner, 2011a, p. 48, 89–144] Related steps, strategies, and methods are discussed later.

5.1.3 Moving Target of Security

Everything can be compromised. Everything can be hacked. It is just a matter of time. Everything is vulnerable after enough time has passed. That is why a control system can not be trusted 100% at any time. It must be assumed that the protections in a control system can be penetrated and bypassed, thus allowing hazardous references passed into the equipment, the AC drive.

For all sorts of embedded and general purpose software, new exploits are published almost every day. New vulnerabilities are found constantly. That means, that a system which is secure today, most certainly is not secure some time from now, unless proper patches are applied. A secure system is the target, but as time goes by, more effort is required to reach that target, the secure system. That is what the concept of *moving target* means in computer security. As Gollmann [2011, p. 1] expressed it: "Security is a journey, not a destination."

The Debian Project, responsible for the free Linux distribution (distro), states the following: "Experience has shown that 'security through obscurity' does not work. Public disclosure allows for more rapid and better solutions to security problems." [Software in the Public Interest, Inc., 2012a] According to the *full disclosure* principle, there are many free sources to vulnerabilities and exploits, including *Exploit Database* (`www.exploit-db.com`) by Offensive Security [2012], the *Bugtraq mailing list* (`www.securityfocus.com`) by Symantec Corporation [2012a], *The Open Source Vulnerability Database* [2012] (`http://osvdb.org/`), and *National Vulnerability Database* (`http://nvd.nist.gov/`) by National Institute of Standards and Technology [2012], to name a few.

5.1.4 The Threat

It is evident, that industrial applications such as the decanter centrifuge are usually susceptible to sabotage and physical destruction, in addition to the common target for traditional hacking, which is "information" theft or leakage. Andress and Winterfield [2011, p. 29–31] present rankings for different types of cyber threats, naming "APT/Nation state" as the worst kind of threat in terms of damage caused. Cyberwar requires resources, like knowledge, tools, and developers.

Mainly free tools available for everyone to download are used in the experimental part of this thesis (Section 7). In that sense, in relation to the tools (described as "logical weapons" by Andress and Winterfield [2011, p. 83]) used, this thesis basically assumes a "script-kiddie" level threat. It is the least damaging type of threat.

On the other hand, the target, a decanter centrifuge used in nuclear fuel production, is relatively high profile and possibly rated as *critical infrastructure* (discussed more later in Section 5.2.4). Considering the industrial nature of the target, the

threats are more serious, in the top range between terrorism, insiders, and APTs or nation states.

The attackers behind Stuxnet obviously had extensive knowledge of the uranium enrichment process with gas centrifuges. They also had insider knowledge about PLC configuration, among other things [Falliere et al., 2011, p. 3]. Thus to protect an industrial application, it must be assumed that a potential attacker attempts to target the "vulnerabilities" of the application.

Speaking in the language of information security, the maximum speed limit of a rotating machinery, such as a centrifuge, is a vulnerability which cannot be patched (i.e. fixed). It is inherent to the design (due to physics). Thus, "a firewall", e.g. an external safety module, is needed to prevent access to the vulnerable area of the system. (Industrial safety implementations are further discussed later in Section 5.4.)

Usually loss of electric power (blackout) is not a threat to an industrial drive application, if only the potential physical damage to the equipment is considered. Most applications withstand an uncontrolled (coast) stop. Although the loss of power is a major threat to a production process, as no production can proceed if there is no power to run production lines in a factory or other facility.

With the increased complexity of AC drives and their programming possibilities it is possible to target them like Stuxnet targeted Siemens S7 PLCs. In the future, we might see a Stuxnet-like malware which modifies user applications running on AC drives through the PC programming tool interface, for example.

5.1.5 Defense-in-Depth

Defense-in-depth is an IS "strategy" using multiple layers of different methods, such as physical protection (door locks, etc.), strong user passwords, and data encryption [Knapp, 2011, p. 23]. If one layer can be penetrated by an attacker, there is another one waiting and still protecting the target. The more layers, the better. For example, if security measures in a PLC have been bypassed and the PLC has been compromised, an AC drive can still protect the application machinery, as long as its protection functions are working and secured.

Byres and Cusimano [2010] write about the similarities of defense-in-depth of IS industry and *layer-of-protection analysis* (LOPA) of automation industry. According to Boyes [2012], that is "a relatively new concept" intertwining security and safety together. It requires co-operation between IACS and IS vendors. However, a vendor with a secure product affects only 25% of total security, while 75% is up to the end-user through policies and training.

Of course, it is easier for a manufacturer of a device with traditional fieldbus connectivity to throw in the towel and say the fieldbus was never intended to implement security. Another way to handle the situation is to make everything possible to improve security. However, [Langner, 2011a, p. 163–164] points out that vendors have very limited possibilities to charge more for the added cybersecurity. After all, it is invisible to the user in many aspects.

As previously discussed in Section 4.2.6 (on page 27), decanters can be inte-

grated into a larger automation system. Remote monitoring and control is truly "a double-edged sword". It brings great benefits, but unless security is taken care of, it bears the potential for a catastrophe. The following subsections discuss security of networked environments common to many industrial remote control and monitoring implementations.

5.2 Industrial Network

Figure 11 presents a diagram of a typical industrial network. It is here only as an example and will not be discussed in detail. Essential points about it to be noted include different kinds of connection possibilities inside and outside the network, and the variety of computers and other devices.

In this thesis, the fieldbus is Ethernet-based. Ethernet per se is not the focus, so it will not be studied in detail. For now, it will only be assumed that the Ethernet network includes usual devices in industrial environment, including PLC, SCADA,

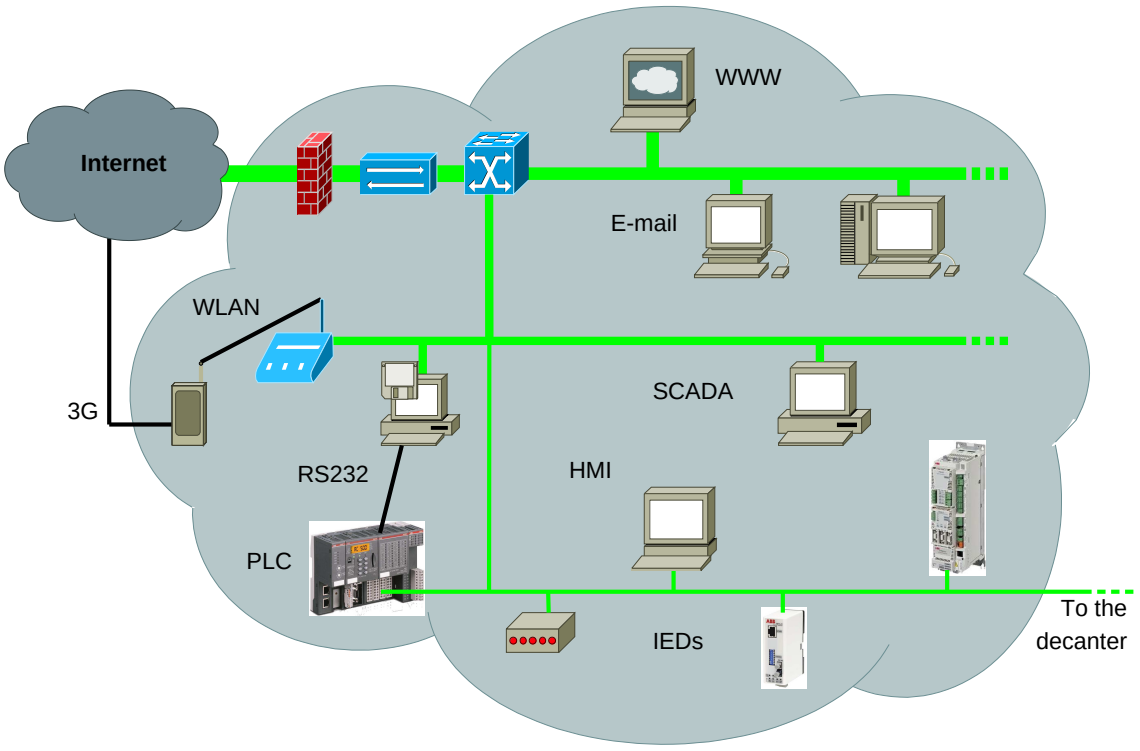


Figure 11: An example case of an Ethernet network for an industrial facility with PLCs, SCADA devices, "business" applications such as world wide web (WWW) browsers, and Internet connections. It should be noted, that a smartphone connected to the WLAN can bypass the Ethernet firewall, possibly linking the industrial network to the Internet, for example through a third generation (3G) mobile broadband network. Devices can be connected also by other means, such as serial communications according to the recommended standard 232 (RS-232). (Adapted from the figure by Knapp [2011, p. 8]. Icons courtesy of Cisco Systems, Inc. [2012]. Photos of the AC500 PLC, the NETA-01 Ethernet module, and the ACSM1 AC drive courtesy of ABB [2012c].)

and "business" devices, as depicted in Figure 11.

5.2.1 Ethernet and Internet Protocol

Ethernet is the networking technology standardized in the Institute of Electrical and Electronics Engineers (IEEE) standard 802.3 [Reynders and Wright, 2003, p. 43–44]. The Ethernet packet with the basic media access control (MAC) frame is presented in Figure 12.

EtherType is "a 2 octet value that indicates the nature of the MAC client protocol." [Institute of Electrical and Electronics Engineers, Inc., 2010, p. 25, 38, 52] It is the *length/type* field of the MAC frame (packet), if the value in the field is greater than 1535. The field is interpreted as the length instead of the type, if the value is less than 1501.

A MAC address, intended to uniquely identify each network device, can be changed. That can be maliciously exploited for *MAC spoofing*. The address resolution protocol (ARP) is used to resolve the MAC address from an Internet protocol (IP) address (IP→MAC). [Sundell et al., 2011, p. 24]

MAC addresses are composed of six 8-bit, hexadecimal values separated by colons, e.g. "00:21:99:00:2D:A9". The first three of those can be used to identify the vendor of the product by the organizationally unique identifier (OUI) list maintained by IEEE. The last three octets are used to identify individual devices. [Institute of Electrical and Electronics Engineers, Inc., 2013, Sundell et al., 2011]

IP (version 4) addresses are composed of four 8-bit, decimal values separated by dots, e.g. "192.168.0.1". Subnet masks (e.g. "255.255.255.0") are required to interpret which portions (number of bits) of the address are used to specify the *subnetwork*, and which the individual devices. Therefore, network segmenting, which is impossible with pure MAC addresses, can be accomplished with IP address filtering (e.g. by firewalls). [Sundell et al., 2011, p. 24]

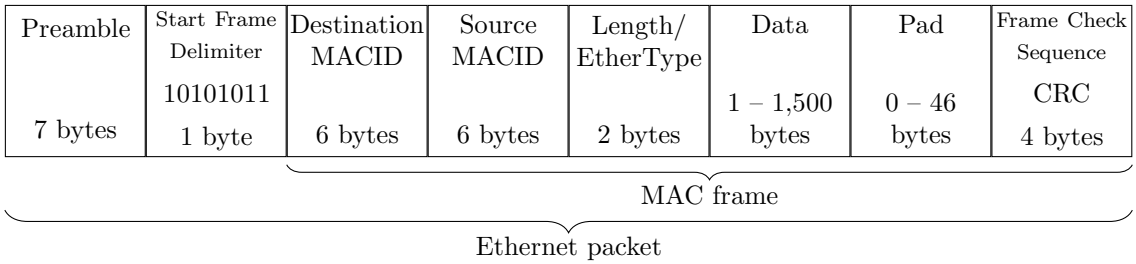


Figure 12: An Ethernet (IEEE 802.3) packet with a basic MAC frame with maximum data field size of 1,500 bytes. A byte is an octet, i.e. 8 bits, transferred starting from the least significant bit. The start frame delimiter (SFD) is always the same sequence of 8 bits. The frame check sequence (FCS) field equals to a 32-bit cyclic redundancy check (CRC) value of the MAC frame. (Adapted from the figures in the works by Reynders and Wright [2003, p. 53], Marshall and Rinaldi [2004, p. 43], and Institute of Electrical and Electronics Engineers, Inc. [2010, p. 49–54].)

5.2.2 Internet Protocol Version 6

With the evolving of the Internet protocol from version 4 (IPv4) to version 6 (IPv6), the IP address space is large enough for every grain of sand on Earth, multiple times [Hagen, 2006, p. 36]. Instead of the less than 4.3 billion 32-bit IPv4 addresses, the IPv6 has 128-bit addresses with $2^{128} \approx 3.4 \cdot 10^{38}$ unique possibilities. IPv6 addresses are written in hexadecimal notation as eight 16-bit values (fields) separated with colons, for example "fe80:43e3:9095:02e5:0216:cbff:feb2:7474". [Frankel et al., 2010, Reynders and Wright, 2003]

Network address translation (NAT), which basically maps multiple IP addresses in a LAN to a single wide area network address, will not be *needed* with IPv6. Nevertheless, NAT can still be used anyway.

IPv6 brings also other new features such as *autoconfiguration*, and mandatory IP security (IPsec) *support* (although use is voluntary) for sender authentication. Frankel et al. [2010, p. 2-7] recommend to deploy at least IPv6 security controls for detecting "unauthorized use" of IPv6, even if there is no intent to replace IPv4.

5.2.3 Industrial Network Security

Knapp [2011] presents several methods for securing networks commonly used in industrial environment, distinguishing them to three major types: the *business network*, the *SCADA demilitarized zone (DMZ)*, and the *control system*. Essential security recommendations are detailed in this subsection.

The terminology Knapp [2011, p. 25–28] uses in his book derives from ICS related standards, such as Critical Infrastructure Protection (CIP) by North American Electric Reliability Corporation (NERC) and ISA99 by International Society of Automation (ISA). Some essential terms are presented below.

Asset "is any device used within an industrial network."

Critical digital asset "is a digitally connected asset that is itself responsible for performing a critical function, or directly impacts an asset that performs a critical function."

Enclave is a "logical grouping of assets, systems and/or services that defines and contains one (or more) functional groups. Enclaves represent network 'zones' that can be used to isolate certain functions in order to more effectively secure them."

Electronic security perimeter (ESP) "refers to the demarcation point between a secured enclave, such as a control system, and a less trusted network, such as a business network." [Knapp, 2011, p. 313–315]

Update of web (hypertext transfer protocol, HTTP) servers and other components can break functionality of industrial applications. Therefore, quick and simple update of any ICS related software is not possible, but requires planning and testing in advance, and also a backup plan, for example the possibility for a rollback in case

things do not work as expected after the update. Information security is balancing between a working process (ongoing production) and security. Everything can not be updated as soon as a patch is available, because it would cause disruptions to the process. As unpatched assets will be present, compensating measures should be established. [Knapp, 2011, p. 281]

The two common IS axioms presented by Knapp [2011, p. 310] should be remembered: "Security is a Process, not a Product" and "Every door is a back door." Knapp [2011, p. 304–305] makes notes about mobile devices plugging into the company WLAN. For example, nowadays it is common for mobile phones to have built-in Wi-Fi (IEEE standard 802.11). This annihilates the air-gap, if any, by connecting the industrial LAN to a wide area network. Another major security threat are misconfiguration and configuration weaknesses, which account for 16% of exploits in ICS, according to a study completed in 2010. One common misconfiguration is the use of default accounts and passwords.

Consequently, Knapp [2011, p. 32] states that "the air gap no longer exists". Critical systems can be found and exploited due to this.

Knapp [2011, p. 125] writes that the business network "should be treated as if it were already compromised." Securing an industrial network starts with identifying functional groups of devices and systems. After that, enclaves can be established. They must be separated from each other with very strict firewall rules, based on the "deny all" default policy. Only specific connections (with source, target, and protocol details) absolutely required should be added as exceptions. This results to strong electronic security perimeters between the enclaves. [Knapp, 2011]

After the enclaves and ESPs have been established, they need to be monitored internally, i.e. traffic within an enclave, and externally, i.e. traffic across an ESP. According to Knapp [2011, p. 204], illegal process manipulation can be detected by an "Application Monitor" or an "Industrial Protocol Monitor", which has a list of authorized function codes/commands. Knapp [2011, p. 272] recommends *whitelisting* with application traffic monitoring to detect "malware operating covertly inside of other applications" (e.g. Stuxnet).

Application whitelisting (AWL) is a host security approach different from traditional anti-virus solutions, which are based on a "blacklist" with a list of "bad" objects. Knapp [2011, p. 185] writes that "AWL is well suited for use in control systems, where an asset should have explicitly defined ports and services." Contrary to blacklisting, AWL does not require constant updating (of malware "fingerprints" or signatures) and is able to block yet unknown, to be discovered (i.e. *zero-day*) attacks or exploits. The downside of AWL is that it adds latency to every function on a host, which may not be approved for time-sensitive applications.

Log collection and analyzing for getting comprehensive view of network activity, and especially detecting unusual activity, is important but often overlooked security feature. Security information and event management (SIEM) systems are recommended for this. The network logs need to be archived, potentially for fulfilling regulations depending on the type of the facility. The archived logs can require large amounts of space, for example 2 *petabytes* for 7 years, according to Knapp [2011, p. 242–244].

Finally, Knapp [2011, p. 303] presents "common pitfalls and mistakes", describing complacency as "one of the most common and dangerous mistakes". It can result from being too confident about existing security solutions, or on the other hand, not taking threats seriously.

5.2.4 Critical Infrastructure Protection

Critical Infrastructure Protection is a "reliability standard" by North American Electric Reliability Corporation [2012]. It contains nine sections numbered as CIP-001–CIP-009. The first one is titled *Sabotage Reporting*, and the rest with the *Cyber Security* prefix as follows: *Critical Cyber Asset Identification*, *Security Management Controls*, *Personnel & Training*, *Electronic Security Perimeters*, *Physical Security of Critical Cyber Assets*, *Systems Security Management*, *Incident Reporting and Response Planning*, and *Recovery Plans for Critical Cyber Assets*.

North American power generation facilities must comply with the NERC CIP under penalty of a fine [Knapp, 2011, p. 13]. Although the decanter is not used in power generation and therefore does not have to comply with the NERC CIP, it is good to take note of the security procedures in other industries. Described in Section 5.2.3, the security measures presented by Knapp [2011] are in accordance with the NERC CIP.

Nevertheless, a decanter plant can be regarded as critical infrastructure, depending on the process. At least the U.S. definition for critical infrastructure is so loose that it can be applied to many industrial facilities. Ultimately defined in the U.S. *Critical Infrastructures Protection Act of 2001* [Office of the Law Revision Counsel, 2012, Title 42 § 5159c (e)], "the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The previous definition is shared by U.S. Department of Homeland Security [2003] in *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, which lists different sectors requiring vulnerability assessments and risk management strategies against attacks. Included among those infrastructure sectors are water treatment systems, and energy production and refining.

5.2.5 Overview of Cybersecurity

Published by International Telecommunication Union [2008, p. 1] (ITU), the recommendation ITU-T X.1205 *Overview of cybersecurity* provides taxonomy of cyber threats at various network layers. Also, "the most common hacker's tools of the trade are presented." These include techniques and methods such as IP spoofing, network sniffing, denial-of-service (DoS) attacks, and eavesdropping among many others. Due to being a *recommendation* instead of a *standard*, compliance with ITU-T X.1205 is voluntary.

According to International Telecommunication Union [2008, p. 8]: "Cybersecurity requires risk management." For benefit of the risk analysis, attacks are grouped into three categories: service interruption attacks, assets compromise, and component hijacking. Attacks in the first category prevent user access either temporarily or permanently, e.g. DoS or distributed denial-of-service (DDoS) attacks. Assets compromise involves "theft or misuse of infrastructure". Component hijacking results to attacks against other parts of "the cyber environment" through devices which the attacker has gained control to. Similar issues are further discussed next in relation to field devices.

5.3 Field Devices and Fieldbus

Electronic devices scattered around a factory floor (a production plant) are usually called *field devices*. They communicate with other devices and systems through a *fieldbus*. This subsection discusses security aspects related to field devices and Ethernet-based fieldbus protocols.

5.3.1 Automation Model

AC drives belong inside the "sacred ground" of the *control system*, as expressed by Knapp [2011, p. 127]. An AC drive is an intelligent electronic device (IED) after a PLC, in the network topology of a control system.

Figure 13 presents the Purdue enterprise reference architecture (PERA) model. According to Macaulay and Singer [2012, p. 89–92], the PERA model "has been

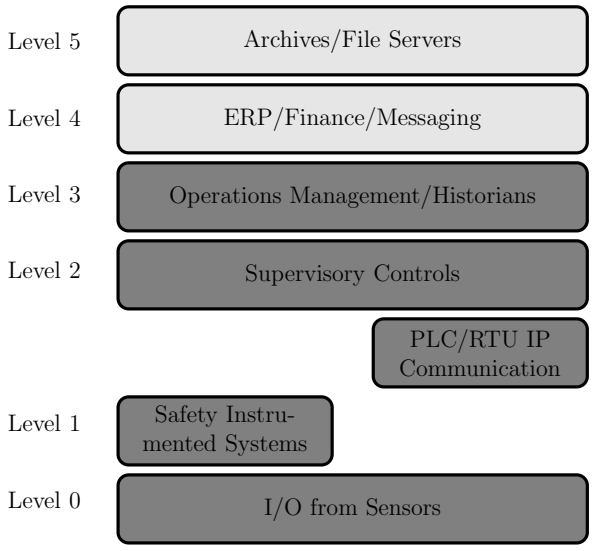


Figure 13: The Purdue enterprise reference architecture (PERA) model. Levels 5 and 4 describe IT systems such as enterprise resource planning (ERP), levels 3 and below ICS systems such as remote terminal units (RTUs). Availability requirement increases from top to bottom, with level 0 having the highest availability requirement. (Adapted from the figure in the book by Macaulay and Singer [2012, p. 92].)

adopted by the ICS community and International Society of Automation (ISA) for representing and designing the interface between ICS and IT." It has six levels, from 0 to 5, depicted in Figure 13. Level 0 includes motor controls. So, AC drives can be assumed belonging to level 0.

An AC drive is the last possible line of defense in the chain of devices controlling a decanter centrifuge. It is the device that feeds power into the electric motor to make it rotate. If all fails, all "upper" control systems have failed and cannot be trusted any more, the AC drive and the safety functions in it are the last resort (apart from completely isolated safety devices and systems).

5.3.2 Security

Sundell et al. [2011] present security aspects of fieldbuses and related devices. Some selected points are summarized in this subsection.

According to Sundell et al. [2011, p. 14]: "The word 'attack' commonly means the deliberate realization of a threat against a system, with the purpose of evading or circumventing security measures and violating security policies." Fieldbus *communication* between devices can be attacked in several ways, including

- man-in-the-middle attack by compromising a gateway, a switch, or a server
- DoS attack by overloading the fieldbus leading to *exhaustion of resources*
- spoofing by exploiting protocols and systems without source or destination address authentication
- disrupting the electrical signals on the physical layer. [Sundell et al., 2011, p. 16–17]

Sundell et al. [2011, p. 16] point out the importance of protecting master devices to prevent an attacker issuing commands to slaves. Also, if safety related fieldbus communications are used, the safety of a process might be compromised in an attack. That especially holds true in systems with functional safety entirely implemented by the automation system.

Originally, traditional fieldbuses were designed to be closed networks. One of the key issues with a fieldbus network is physical security. For example, devices distributed across a plant might not have protective enclosures, which presents a security risk for an insider attack. Also, unused ports can be an intrusion point into the network, especially with Ethernet. [Sundell et al., 2011, p. 16, 26, 31]

According to Sundell et al. [2011, p. 32], field *devices* can be manipulated in two ways: "through the PC software" or using "integrated user interface such as keypad and display." The manipulation can be device parameter changes, or inserting "spoofed firmware updates" which are usually "encrypted with a symmetric key". Potentially, the encryption key can be found from the memory of a field device.

To protect device parameters against modification, user access levels with passwords can be defined. Furthermore, the passwords should be securely stored, preferably with encryption. Also, firmware updating needs to be secure. Illicit firmware

modifications can be detected by error checking algorithms in a bootloader. It is not enough that the firmware is encrypted—proper key management is also needed. [Sundell et al., 2011, p. 37]

Regarding the security of operating systems, Sundell et al. [2011, p. 34] state that by experience "all kinds of operating systems have vulnerabilities regardless of open source or closed source."

5.3.3 EtherNet/Industrial Protocol

EtherNet/IP is developed by Open DeviceNet Vendor Association (ODVA). Introduced in 2001, it implements the Common Industrial Protocol (CIP) over standard Ethernet. The "IP" in EtherNet/IP does not stand for "Internet Protocol", but for "Industrial Protocol" instead. Nevertheless, EtherNet/IP employs the transmission control protocol with the Internet protocol (TCP/IP). [Open DeviceNet Vendor Association, Inc., 2008, p. 5]

Two types of communication modes are supported by EtherNet/IP, which uses standard Ethernet frames (with EtherType 0x80E1): client/server, and real-time "implicit" mode, which uses connectionless transport by the user datagram protocol (UDP) and multicast transmissions. Objects standardized by CIP define qualities of devices: *Required Objects* include device identifiers, like the manufacturer and the serial number, while *Application Objects* define input and output profiles. There are also *Vendor-specific Objects*. [Knapp, 2011, p. 78–79]

According to Knapp [2011, p. 79], there are multiple security concerns specific to EtherNet/IP, mostly introduced by CIP, including: no security mechanisms are defined, devices can be easily identified through the common Required Objects, and real-time UDP and multicast traffic can be spoofed. Due to those security issues, it is recommended to use intrusion detection system (IDS) or intrusion prevention system (IPS) suited for SCADA applications (SCADA-IDS/IPS) capable of detecting and interpreting the real-time EtherNet/IP protocol. Also, the general industrial network security measures (presented in Section 5.2.3), e.g. strong perimeter security controls, should be implemented. [Knapp, 2011, p. 79]

According to the ICS-CERT [2012b] alert on February 15, 2012, there is an exploit for the EtherNet/IP protocol, which makes it possible to crash devices. The alert followed publication by Project Basecamp of Digital Bond, Inc. [2012a], including a Metasploit module with four payloads. Two of those payloads are targeting protocol stack errors in the ControlLogix PLC by Rockwell Automation / Allen-Bradley (AB), but they will also affect *any device* using the same protocol stack. More importantly, according to Digital Bond, the other two payloads are effective against *any EtherNet/IP device* from approximately 300 vendors of ODVA, including 3S-Smart Software Solutions GmbH and ABB, Inc. [Open DeviceNet Vendor Association, Inc., 2012].

According to Digital Bond, Inc. [2012a], the EtherNet/IP protocol is "insecure by design", as request commands are not authenticated, allowing operations such as "Stop CPU" and "Reboot Ethernet Controller". Digital Bond has verified that a device from ABB (model unspecified) is vulnerable to this, as the extra security

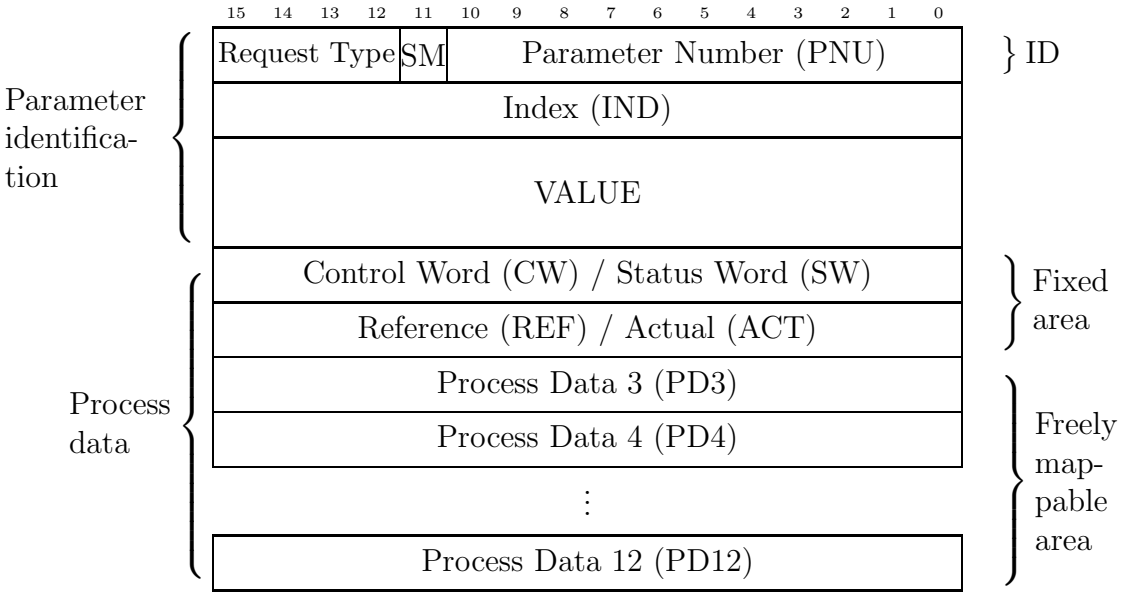


Figure 14: A PROFIBUS frame (data unit part of the PROFIBUS SD2 telegram) with the two main sections: the parameter identification and the process data. Parameters of AC drives can be changed by the PROFIBUS master (usually a PLC) using the parameter identification section. The meaning of the fixed fields of the process data differs depending on the sender of the frame: The master sends control words and references, while slaves respond with status words and actual values. The number of process data (PD) fields in the freely mappable area (0–10) depends on the parameter/process data object (PPO) type. The SM field for the request signal is not used (value of 0). [ABB Oy, 2011a, Falliere et al., 2011]

step of authentication is not required. [Roberts, 2012]

5.3.4 Process Field Network—PROFINET

Process field network (PROFINET) is the modular communication standard developed by PROFIBUS & PROFINET International. It is basically integration of the process field bus (PROFIBUS) with the full-duplex Ethernet at 100 megabits per second (Mbit/s). The number of PROFINET devices has been increasing since 2002, currently being over four million. The PROFINET IO protocol, with the distributed I/O data perspective, was standardized (standard 61158) by International Electrotechnical Commission (IEC) in 2004. [Åkerberg and Björkman, 2009, PROFIBUS Nutzerorganisation e.V., 2011, 2012]

PROFINET is a real-time Ethernet protocol (with EtherType 0x8892) with master/slave communication. Multiple masters are supported by token sharing, while each slave can respond to a single master. [Knapp, 2011, p. 80]

The structure of the PROFIBUS frame used in master/slave communication is depicted in Figure 14. Parameters of AC drives can be changed through the PROFINET fieldbus by "requesting" change of a parameter value, to which the slave (the AC drive) responses with an acknowledgment. The drive can be started

and stopped through the control word field, and the speed (reference) is set through the REF field. [ABB Oy, 2011a, p. 116]

PROFINET IO cyclic data messages are addressed by MAC addresses. UDP is used for acyclic communication with IP addressing. [Sundell et al., 2011, p. 29]

To address the numerous security concerns of PROFINET, such as inherent lack of authentication, Knapp [2011, p. 80] recommends strong isolation using firewalls and IPS devices, in accordance with the other network security recommendations (described in earlier Section 5.2.3).

Siemens SIMATIC S7 range of PLCs with PROFINET connectivity use the International Standards Organization transport service access point (ISO-TSAP) protocol for communication and programming with the related "engineering software". According to Langner Communications GmbH [2011], on top of the ISO-TSAP protocol, Siemens uses an application layer proprietary protocol called the *S7 protocol*. Due to security flaws in the implementations of these protocols, SIMATIC S7 PLCs can be compromised with root shell (command prompt) access to their (x86) Linux OS, among other malicious things. [Beresford, 2011, p. 5, 19]

5.4 Machinery and Process Safety

This subsection focuses on machinery and process safety systems, generally known as safety instrumented systems (SIS).

5.4.1 About Safety Instrumented Systems in General

Knapp [2011, p. 35] recommends to consider safety and security independently of each other. But in this thesis, safety is considered to be a security enhancing feature. Also Langner [2011a, p. 134] points out that "safety systems are one more way to increase the robustness of a process". Actually, functional safety features are intended for the protection of human beings [International Electrotechnical Commission, 2005, p. 7].

Traditionally, safety systems have been isolated from any remote control systems. Nowadays, it is common that safety devices can be remotely monitored, along with the rest of the field devices. [U.S. Department of Homeland Security, 2009, p. 17, 20] Integrated safety solution, such as functional safety of an AC drive (presented in the next subsection), utilizing a single (Ethernet) fieldbus wiring offers advantages over traditional hardwired and separate safety systems: "reduced design, installation, and maintenance costs, as well as expanded diagnostic capabilities." [Cisco Systems, Inc. and Rockwell Automation, Inc, 2011, p. 2–3]

Industrial standards and other related documents recommend separating process control and safety/protection systems (Figure 15). (Safety systems are also called "interlock systems".) For an AC drive application, that means that there should be separate safety devices, whether or not safety functions of the AC drive are used. Exception to this is to design the whole system as "a safety-related system". Justifying non-conformity with standards on economical grounds might not look

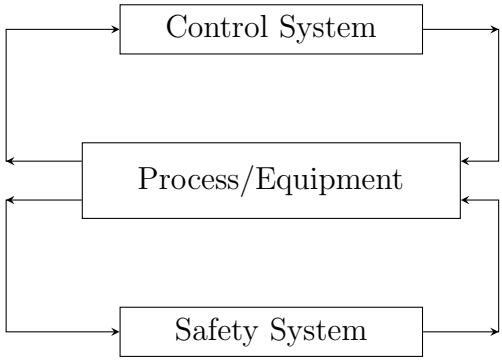


Figure 15: Principle of separated control and safety systems. (Adapted from the figure in the book by Gruhn and Cheddie [2006, p. 38].)

good in a court of law, if it ever comes down to that. [Gruhn and Cheddie, 2006, p. 37–45]

Safety instrumented systems are a part of industrial control systems (ICS). Macaulay and Singer [2012, p. 14] state the following: "Understanding the purposes and function of SIS is critical to managing the security of ICS." Furthermore, a common fallacy is to assume that ICS does not need additional security measures due to SIS. However, SIS often share the technology platform with ICS, for example using the same Windows application to configure both systems, and they need to be connected somehow for proper monitoring and invoking. Therefore, there is no such thing as a "disconnected safety system". Because of these issues, an attacker can compromise, bypass, or suspend a safety logic. [Macaulay and Singer, 2012, p. 14–15]

According to Macaulay and Singer [2012, p. 15]: "There are currently a number of private and closed source studies being conducted on the security of SIS, and it is likely that more information will be available publicly in the coming months and years." This thesis can be regarded as a study on the security of SIS implemented with the functional safety features of AC drives.

Stuxnet has demonstrated that protection functions, which can be disabled directly through the fieldbus, can not be trusted. (Section 3.4.1 describes the protection functions of AC drives disabled by Stuxnet through PROFIBUS.) Therefore, a safety system, which is more secure, is required for protection against a Stuxnet-like threat. One kind of safety system, which can be implemented with AC drives, is presented in the next subsection.

5.4.2 Functional Safety

Applicable to AC drives, the international standard IEC 61800-5-2 *Adjustable speed electrical power drive systems—Part 5-2: Safety requirements—Functional* by International Electrotechnical Commission [2007] shares the definition for *functional safety* from the IEC 61508-4 standard as follows:

Functional safety is "part of the overall safety relating to the EUC (equipment under control) and the EUC control system which depends on the correct func-

> tioning of the E/E/PE (electrical/electronic/programmable electronic) safety-related systems, other technology safety-related systems and external risk reduction facilities" [International Electrotechnical Commission, 2007, p. 12].

Functional safety features are usually implemented in a PLC or in an AC drive. In this thesis, PLC equipment are not studied and therefore all safety functions presented later are internal to the AC drive itself. International Electrotechnical Commission [2007, p. 13] refers to this kind of equipment as "adjustable speed electrical power drive system suitable for use in safety-related applications" (PDS(SR)).

The safety functions standardized by International Electrotechnical Commission [2007, p. 16–18] are described in Appendix A (on page 115). Comparing them to the vulnerabilities of decanters, previously discussed in Section 4, many of them seem useful, especially the following functions: safe acceleration range (SAR) to prevent slippage of the belts (discussed in Section 4.3.3), safe speed range (SSR) to protect the bowl against excessive speeds and also to keep the separation/dewatering process (production) running by preventing the speed dropping too much (discussed in Section 4.2.4), safely-limited torque (SLT) to protect the gearbox (discussed in Section 4.2.4), and safe motor temperature (SMT) to protect the main motor against overheating during long accelerations (discussed in Section 4.3.3).

However, not all of those applicable safety functions are actually implemented in real AC drive products. Therefore, the amount of available safety functions is considerably limited in real life, as will be presented later.

Safe torque off (STO) is central to many functional safety implementations. It is used to prevent electromagnetic torque in a motor. Generally it is achieved by directly cutting off the gate signals to IGBTs. Gate signals control IGBTs and without them an IGBT can not switch on. [ABB Oy, 2012e, International Electrotechnical Commission, 2007, Rockwell Automation, Inc., 2012k, Siemens AG, 2011b]

According to ABB Oy [2012e, p. 169, 175]: "The Safe torque off function is ineffective against deliberate sabotage or misuse." However, in this thesis the STO function will be harnessed against *cyber sabotage* as an additional layer of defense-in-depth security strategy.

With the defense-in-depth concept (presented Section 5.1.5) in mind, it is easy to see how a functional safety system of an AC drive could be the last defensive method against cyber sabotage. For traditional sabotage, the target is always some physical equipment. A decanter centrifuge needs multiple layers of protection to prevent physical damage to it, in case of a serious cyber sabotage attempt (cyber-physical attack).

5.4.3 Speed Feedback for Safety Functions

Some implementations of the safety functions require speed feedback from the (rotating) axis of the motor. Feedback devices are usually called *tachometers* or (rotary) *encoders*, as they "encode" the speed and/or position information to a machine readable form. There are many types of encoders or feedback devices.

Roughly speaking, encoders can be divided into two categories: incremental and absolute. The incremental encoder does not know the exact position of the rotor,

only the amount it has been rotated, unlike the absolute encoder. Rotation is indicated by digital pulse signals, typically with transistor-transistor logic (TTL) or high threshold logic (HTL) voltage levels (nominally +5 V or +24 V, respectively), or analog sine/cosine (Sin/Cos) signals. Absolute encoders keep track of the actual position of the rotor, and can return that information generally at any time through a digital interface, such as synchronous serial interface (SSI), encoder data (EnDat), or Hiperface.

The price for a tachometer can be substantial, even a four figured number in U.S. dollars [Alibaba.com Hong Kong Limited, 2012]. Several encoders might be required, depending on the application. To reduce costs, a machine builder might prefer a solution without an encoder, if speed feedback is not an application requirement otherwise. The feedback types supported by actual AC drives are discussed later (in Section 7.3.1).

Unlike Europe, the United States of America (USA) does not have machinery safety legislation applicable to the whole region [Siemens AG, 2011b, p. 338]. Some European safety standards related to decanter centrifuges and AC drives are discussed in the following subsections.

5.4.4 Common Safety Requirements for Centrifuges

The European standard EN 12547:1999+A1 *Centrifuges—Common safety requirements* is a class C standard "dealing with detailed safety requirements for a particular machine or group of machines", as defined in the European standard EN ISO 12100:2010 by Comité Européen de Normalisation [2010, p. vi] and International Organization for Standardization (ISO). It applies to decanters which are a certain type of centrifuges. EN 12547 provides "a means of conforming to Essential Requirements" of the *Machinery Directive* (EU 2006/42/EC). [Comité Européen de Normalisation, 2009]

The European standard about safety of centrifuges lists hazards "normally associated" with the usage of centrifuges, including maintenance and cleaning, and safety measures to cope with those hazards. The list of hazards "is the result of a risk assessment carried out in accordance with" the standard EN 1050 *Safety of machinery—Principles for risk assessment*. From the perspective of this thesis, the most essential hazardous events are "Failure/disorder of the control system" and "Break-up during operation". [Comité Européen de Normalisation, 2009, p. 9, 28]

The standard EN 12547 requires "a speed control and an overspeed prevention device" to protect against mechanical hazards, such as rotor rupture, if an AC drive is used to drive a centrifuge. Such "overspeed protection system" is defined as "a safety related part." Those safety parts of the control system "shall be designed in accordance" with the standard EN 954-1 *Safety of machinery—Safety related parts of control systems—Part 1: General principles for design*, which has been superseded by the European Standard EN ISO 13849-1 (described in the next subsection). The "fault resistant category of safety related parts" should "preferably" be 1 or 2, depending on the part. For example, speed control should be category 2, and safety related stop 1 *or* 2. [Comité Européen de Normalisation, 2009, p. 11, 17–18]

5.4.5 Safety-Related Parts of Control Systems

The European standard EN ISO 13849-1 *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design (ISO 13849-1:2006)* by Comité Européen de Normalisation [2008, p. v] is a type-B1 standard dealing with particular safety aspects, for all kinds of machinery. It is intended to provide guidance for design and assessment of control systems to fulfill the "Essential Safety Requirements" of the *Machinery Directive* (European Council Directive 98/37/EC). In addition to design considerations, the EN ISO 13849-1 standard mainly discusses safety functions, which can be provided by the safety-related parts of control systems (SRP/CS), and categories (B, 1, ..., 4) used to achieve a specific performance level (PL, a–e) which corresponds to the ability to perform a safety function. [Comité Européen de Normalisation, 2008]

As either a separate system or integrated into the machine control system, SRP/CS provide safety functions and possibly operational functions also. They consist of hardware and software. [Comité Européen de Normalisation, 2008, p. v] The EN ISO 13849-1 standard borrows the following definition from the ISO 12100-1:2003 standard:

Safety function is a "function of the machine whose failure can result in an immediate increase of the risk(s)". [Comité Européen de Normalisation, 2008, p. 5]

The functions described in IEC 61800-5-2 (previously discussed in Section 5.4.2) facilitate implementation of the principles of EN ISO 13849-1 [International Electrotechnical Commission, 2007, p. 8].

The standard lists PLCs and "motor control units", among others, as examples of devices "which are parts of SRP/CS" [Comité Européen de Normalisation, 2008, p. 1]. Specific requirements for those kinds of *programmable electronic systems* are provided, however, EN ISO 13849 applies also to SRP/CS utilizing other forms of energy than electricity, e.g. hydraulic, pneumatic, or mechanical energy. [Comité Européen de Normalisation, 2008, p. 1]

According to Comité Européen de Normalisation [2008, p. 11], performance levels (PLs) correspond to value ranges of "average probability of dangerous failure per hour" in decreasing order from PL a with values less than 10^{-4} to PL e with values less than 10^{-7}. Performance levels b–e can be related to safety integrity levels (SILs) 1–3 [Comité Européen de Normalisation, 2008, p. 16].

EN ISO 13849-1 also manifests requirements for software used to configure safety-related parameters. The parameterization tool needs to be dedicated software with identification information, such as a name and a version, and prevention of unauthorized modification, for example a password. Furthermore, Comité Européen de Normalisation [2008, p. 26] states the explicit requirement for "verification that unauthorized modification of safety-related parameters is prevented". However, further security requirements, such as password complexity, are not given. [Comité Européen de Normalisation, 2008, p. 25–26] In the next section, parameterization tools for safety-related parameters from selected vendors are introduced, among other things.

6 Selected AC Drives and Software Tools

This section describes the AC drives selected for comparison, and the software tools used with them. Essentially, they constitute the materials for this thesis, apart from the literature introduced earlier. Firstly, the physical AC drives are presented along with reasons for their selection, followed by the PC software tools used to commission and configure them. Finally, the tools for vulnerability assessment are described.

6.1 AC Drives

The AC drives selected for the comparison are presented in this subsection. First, the selection process and criteria are explained, then the individual drives are introduced to the reader.

6.1.1 Drive Selection

Different AC drives were chosen for comparison based on the decanter/centrifuge application requirements. Drive offerings from different manufacturers were studied, and the drive model with suitable power, connectivity, and safety features was chosen

Table 2: Technical details of the selected AC drives including the option modules. I_N and I_{max} are the nominal and the maximum output currents, respectively. P_N is the nominal output power and $P_{N(max)}$ the maximum offered for the same "frame type" (i.e. size named by the manufacturer). Dimensions are presented as height x width x depth in mm. S110 is a modular drive comprised of the PM340 power module (1.2 kg) and the CU305 PN control unit (1.0 kg), supplied separately. [ABB, 2011b, 2012d, ABB Oy, 2012e, Rockwell Automation, Inc., 2009, 2011, 2012b, Siemens AG, 2008, 2011a,c, 2012a,h]

Manufacturer	ABB	Rockwell	Siemens
Model	ACS880-01-02A4-3	AB PowerFlex 755	SINAMICS S110
U_N (V)	400	400	400
P_N (kW)	0.75	0.75	0.75
I_N / I_{max} (A)	2.4 / 3.1	2.1 / 3.2	2.2 / 4.4
Frame type	R1	2	FSA
$P_{N(max)}$ (kW)	5.5	11	1.5
Dimensions	405 x 155 x 226	424 x 134 x 212	195 x 73 x 216
Weight (kg)	6	8	∼2.2 (1.2+1)
Fieldbus connectivity	EtherNet/IP, Modbus TCP, PROFINET IO	EtherNet/IP	PROFINET
Option modules included	FENA-11 Ethernet, FEN-11 Encoder, FSO-11 Safety	20-HIM-A6 Panel, 20-750-UFB-1 Feedback, 20-750-S1 Safe Speed Monitor	BOP20 Panel, Safety Integrated Extended Functions
Introduced	April 2011	November 2009	November 2008

from each selected manufacturer. Two manufacturers in addition to ABB were first chosen based on the safety features presented in their marketing materials (catalogs, web sites, etc.). The two manufacturers with the most extensive safety feature offering were selected. Biggest AC drive manufacturers by market share were compared for this.

An AC drive for a decanter or a centrifuge application was preferred if offered by a manufacturer. Unfortunately, the offerings often lacked other required features, like Ethernet for fieldbus connectivity and safety features. That is why the selected drives, excluding the ACS880-01 from ABB, are generally for motion control applications with position control, which is not needed for a decanter. From an AC drive's perspective, the decanter centrifuge is rather easily controlled with traditional speed and torque control (as previously described in Section 4.4).

Technical details of the chosen AC drives are presented in Table 2. All drives represent the lowest power offered in the product line, which is 0.75 kW for all drives. An actual decanter machinery was not available for the experimental part of this thesis, so the power of the drives does not matter, as they will not be driving real machinery. (For example, the P2 decanter product range by Alfa Laval [2006] is available in powers between 15 to 250 kW.)

6.1.2 Hardware Test Setup

The drives can be seen mounted to the test setup in Figure 16. The Siemens drive has much smaller physical dimensions compared to the other two drives, which can be explained by the maximum power for the frame type offered by the manufacturer (in Table 2). The power range available for the frame type of the Siemens drive is much smaller when compared to the frame types of the other two manufacturers. The kind of power range optimization used in the Siemens drive is typical for *servo drives*, along with built-in feedback device support which is also included in the SINAMICS S110 model.

All three AC drives were coupled to small induction motors. The Ethernet interfaces, configured with static IP addresses (10.0.0.1), were cabled (one at a time) *directly* to a standard laptop PC (configured as 10.0.0.2). No hubs, switches, nor anything else were used in between. This is a drastic difference compared to usual network configuration, where crossover cabling is never used in practice and multiple switches between devices is the norm. However, thanks to automatic medium dependent interface crossover (Auto-MDIX) support, standard Ethernet cables could be and were used.

Also, the distinct PC tool interfaces were used: USB on the ABB ACS880-01 control panel, drive peripheral interface (DPI) through the Rockwell 1203-USB converter adapter, and RS-232 on the Siemens S110 control unit through the Moxa UPort 1450l USB-to-serial converter and a null modem cable. More specific details, such as version numbers and types of different hardware components, are presented in Appendix B.

ACS880-01 was the only AC drive supporting multiple different fieldbus protocols (in the specified configuration). It was configured for EtherNet/IP during the tests.

Figure 16: The three AC drives mounted on the wall, in order from left to right (with dimensions height x width x depth in mm): SINAMICS S110 (195 x 73 x 216) by Siemens AG [2011c], ACS880-01 (405 x 155 x 226) by ABB [2012d], and PowerFlex 755 (424 x 134 x 212) by Rockwell Automation, Inc. [2011]. Only supply cables are wired to the drives.

6.1.3 ABB ACS880-01

The ACS880 is the successor to the ABB's ACS800 AC drive series released in 2002 [DFA Media Ltd, 2002]. The ACS880 series includes different types of drives with different constructions, such as the ACS880-01 wall-mounted and the ACS880-07 cabinet-built single drives. In accordance with the ABB's new low voltage AC drive portfolio introduced in 2011, all of them have common features, such as STO functionality built-in as standard, DTC motor control, a removable memory unit, a drive-to-drive (D2D) link, and optional speed feedback modules and fieldbus adapters.

Dubbed as "all-compatible" industrial drives by ABB [2012d, p. 5], the ACS880 series is intended for several "industries such as oil and gas, mining, metals, chemicals, cement, power plants, material handling, pulp and paper, sawmills and marine." Applications can be, for example, "cranes, extruders, winches, winders, conveyors, mixers, compressors, pumps and fans." [ABB, 2011b, 2012d]

By the optional FENA-11 Ethernet adapter, supported fieldbuses include EtherNet/IP, Modbus TCP, and PROFINET IO. The standard HMI control panel has a mini-B type USB connector for PC tools [ABB Oy, 2012b, p. 20].

ACS880-01 has two built-in registered jack 45 (RJ-45) connectors, but they are not used for any Ethernet based fieldbus communication. Instead, they are used for daisy-chaining the drives together using standard Ethernet cables, to be controlled

by one control panel. ACS880 has ABB's own D2D link built-in. D2D employs RS-485 for inter-drive communication with one master drive and multiple follower drives. [ABB Oy, 2012e, p. 99, 104]

6.1.4 Rockwell Allen-Bradley PowerFlex 755

The Allen-Bradley PowerFlex 750-series AC drives from Rockwell Automation, Inc. [2011] are for general purpose and high performance industrial applications. They are available for 400 - 690 V supplies with powers ranging from 0.75 to 1,000 kW. Standard features include integration with the Rockwell Logix PLC environment, predictive diagnostics, and slot-based architecture for add-ons, such as communications, I/O, and safety options. [Rockwell Automation, Inc., 2011]

The PowerFlex 755 model has an embedded Ethernet port as standard, and allows control of permanent magnet motors in addition to induction motors. It is suited for applications with advanced positioning, offering features like electronic gearing and position/speed profiling, among other positioning features. [Rockwell Automation, Inc., 2011]

In addition to the embedded EtherNet/IP adapter on the main control board, PowerFlex 755 offers Allen-Bradley's DPI which can be used to connect the optional 1203-USB converter for PC tools. As a functional enhancement to AB's SCANport interface, the DPI port in the drive is provided through a (8-pin) mini-*Deutsches Institut für Normung* (DIN, German Institute for Standardization) connector. [Rockwell Automation, Inc., 2012g,h]

6.1.5 Siemens SINAMICS S110

The SINAMICS S110 AC drive from Siemens is a compact servo drive with integrated safety function for basic single-axis positioning applications. According to Siemens AG [2012h], typical applications are the following: "Pick & place tasks, high-bay racking units, simple handling tasks, positioning rotary tables, positioning adjuster and actuator axes in all machinery construction sectors". [Siemens AG, 2012h]

SINAMICS is the name of the "drive family" by Siemens AG [2012h], which includes AC and DC drives for low and medium voltages. As a low voltage AC drive, S110 features servo, speed, and position control for synchronous and induction (servo-) motors. Siemens AG [2011b, p. 129] defines *servo control* as closed-loop control "with a high dynamic response and precision for a motor with a motor encoder." Basically it is high performance, closed loop speed and torque control.

According to Siemens AG [2012h], the following positioning functions are included: "Point-to-point positioning; absolute/relative; linear/rotary axis; flying positioning; traversing blocks (max. 16)". The position control performance is stated as "4 ms". [Siemens AG, 2012h]

As a standard feature, the CU305 PN control unit has two RJ-45 connectors for PROFINET. There is also a third RJ-45 socket for the Drive Component Link with IQ (DRIVE-CLiQ) interface, used to connect an encoder. In addition, all CU305 units have a RS-232 serial interface for PC tools, and a memory card slot.

The memory card itself is optional, but required for the license for safety functions. [Siemens AG, 2011a,b]

6.2 Software for Drives

In the AC drive industry, the term *PC tools* usually refers to software running on Microsoft Windows OS used to commission, program, and monitor the operation of one or multiple AC drives. This subsection presents the PC tools used with the AC drives in this thesis, starting with the motivation for their study.

6.2.1 Vulnerabilities

PC tools of AC drives are similar to the Siemens WinCC software targeted by Stuxnet [Falliere et al., 2011, p. 26–27]. In the last couple of years, many vulnerabilities have been reported in these kind of software used to program PLCs from many different manufacturers (Table 3), as well as in PLCs (firmware) themselves [Digital Bond, Inc., 2012b]. Evidently, the manufacturers of the AC drives compared in this thesis have had security issues in the past. Thus, it is important to study also the vulnerabilities of the PC software of an AC drive. Similarly to the Stuxnet case, an APT or a cyber weapon might target PC tools to configure and program an AC drive directly to its needs for malicious purposes. Although AC drive PC tools are usually needed only once during commissioning, the interfaces and protocols used are available during other times of operation, and can be accessed also by others (unauthorized personnel) unless proper precautions are taken.

ICS Cyber Emergency Response Team (ICS-CERT) works in collaboration with U.S. Computer Emergency Readiness Team, which is a part of the U.S. Department of Homeland Security (DHS). ICS-CERT publishes advisories and alerts about vulnerabilities in industrial control systems to the public. [ICS-CERT, 2010]

Generally, it takes relatively long time from the discovery of a vulnerability to publishing of an advisory or an alert by ICS-CERT. Thus, it can be assumed that

Table 3: Selected alerts and advisories from ICS-CERT [2012c] related to PC tools for PLCs and AC drives, sorted by date (YYYY-MM-DD) in ascending order

Date	ID	Vendor	Title
2010-10-28	ICSA-10-301-01A	Moxa	"MOXA Device Manager Buffer Overflow (UPDATE)"
2011-10-06	ICSA-11-273-03A	Rockwell	"Rockwell RSLogix Denial-of-Service Vulnerability (UPDATE)"
2012-04-06	ICS-ALERT-12-097-02	3S	"3S-Software CoDeSys Improper Access Control"
2012-04-10	ICSA-12-095-01A	ABB	"ABB Multiple Components Buffer Overflow (UPDATE)"
2012-04-18	ICSA-12-030-01A	Siemens	"Siemens SIMATIC WinCC Multiple Vulnerabilities (UPDATE)"

vulnerabilities published by ICS-CERT are widely known, sometimes even before the publication by ICS-CERT, at least in the security community.

However, no publications about possible vulnerabilities in the PC tools presented in the next subsections were found. It does not mean there are none, they just may not have been published yet.

6.2.2 Drive Composer

Drive Composer (Figure 17) is the commissioning tool for ABB's common architecture drives, such as the ACS880-01. As a 32-bit application running on Windows, it allows controlling and monitoring a drive, and changing parameters among other things. More features are available in the Pro version, including control diagrams and safety configuration options, as compared to the limited Entry version. [ABB Oy, 2012b, p. 17]

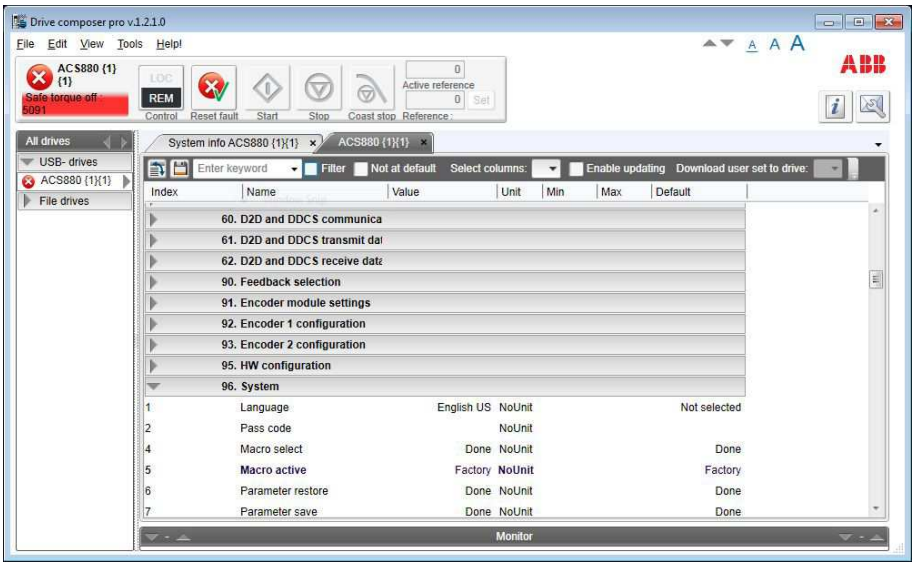


Figure 17: A screenshot of an ABB Drive Composer Pro session, with the parameter browser active, running on Windows 7.

Drive Composer Entry is free, but requires registration with personal information for the download link. At the time of writing, the latest Pro version is 1.2 released on October 30, 2012. [ABB, 2012a]

6.2.3 DriveExplorer

DriveExplorer (Figure 18) is the online configuration and monitoring tool for Rockwell Automation drives, including the PowerFlex 7-Class series. Before becoming obsolete, it was available as the freeware Lite and the chargeable Full versions. Ethernet connectivity was available only in the Full version, in addition to serial connectivity. At the time of writing, the latest version is 6.04.99 released in April, 2012, and runs on Windows XP, Vista, and 7. [Rockwell Automation, Inc., 2012d,f]

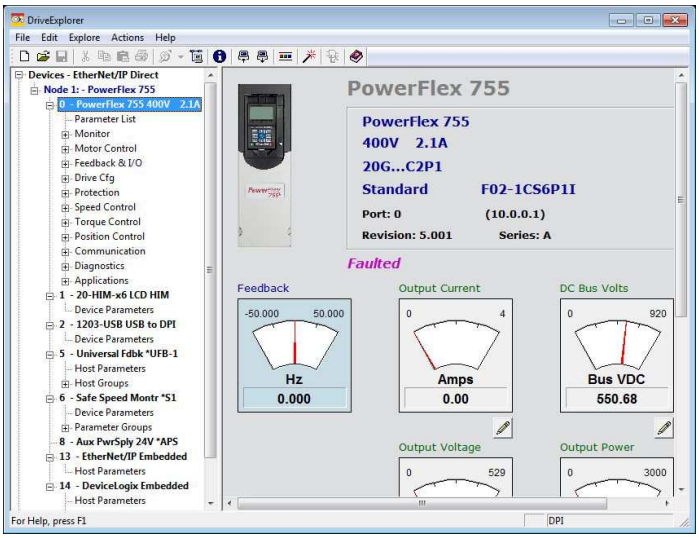


Figure 18: A screenshot of a Rockwell DriveExplorer Full session with the main drive view active.

Originally released in 1998, DriveExplorer has recently been discontinued and replaced by Connected Components Workbench (CCW) released in September 2012. In addition to PowerFlex drives, CCW works as programming and configuration software with variety of devices from Rockwell Automation, including PLCs and HMIs. The supported programming languages are common to any PLC environment (defined in the standard IEC 61131-3): ladder logic, function block diagram, and structured text. CCW is free software available in exchange for registration. Also the latest DriveExplorer Full version (6.04.99) has been released as freeware as a result of becoming obsolete, and can be installed using any serial number. [Rockwell Automation, Inc., 2012d,e]

6.2.4 STARTER

STARTER (Figure 19) is a tool for commissioning, optimization, and diagnostics for Siemens SINAMICS drives. It can be used as a standalone Windows application, or integrated into the other Siemens software: SIMATIC STEP 7 and SCOUT. [Siemens AG, 2011c, p. 14/5]

Advertised as user-friendly by Siemens, STARTER includes project wizards, controller self-optimization, and diagnostics about control/status words and parameters. Additional "SINAMICS Support Packages" are provided for different different AC drive models and features. [Siemens AG, 2011c, 2012f]

At the time of writing, the latest version of STARTER is V4.3 SP1 HF2 released on June 19, 2012. It can be used free of charge without a license key, but ownership of a STARTER license certificate is required for "legal licensing reasons". [Siemens AG, 2012f]

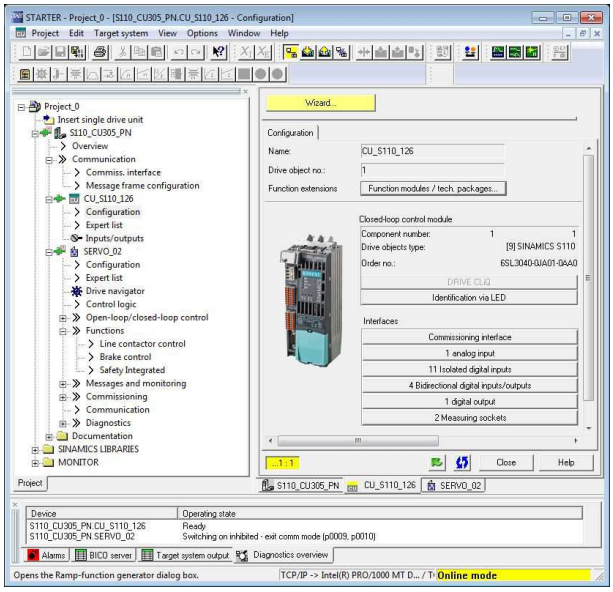


Figure 19: A screenshot of a Siemens (Drive ES) STARTER session with the control unit configuration screen active.

6.3 Vulnerability Assessment Tools

This thesis includes vulnerability assessments of the AC drives. The tools used for that are introduced in this subsection, starting with explanation of motivation for the assessment.

One might question what does vulnerability assessment, traditionally associated with IT equipment, have to do with an AC drive application. If there are vulnerabilities in the firmware of an AC drive, such as a buffer overflow which allows an attacker to perform arbitrary (unrestrained) actions remotely with the AC drive, protection methods can be bypassed and safety functions disabled altogether. Then it does not matter what kind of safety features are implemented. The Stuxnet case has proved that if a safety system (e.g a speed limiter) is integrated into the control system, security affects safety. (Stuxnet disabled the frequency (speed) limitation functions of AC drives, as previously explained in Section 3.4 on page 19.)

6.3.1 VirtualBox

VirtualBox by Oracle Corporation [2012a] is x86 and AMD64/Intel64 virtualization software suite for enterprise and home use. Despite being freely available and open source software, VirtualBox has features and performance comparable to commercial virtualization software.

Offered by Oracle Corporation [2012c] solely through `www.virtualbox.org`, VirtualBox base package (platform) is licensed under the general public license (GPL), but a separate *Oracle VM VirtualBox Extension Pack*, which offers USB 2.0 support for example, is licensed under *VirtualBox Personal Use and Evaluation License*. It allows personal, academic, and product evaluation use free of charge. According to Oracle Corporation [2012b], it is considered *personal use* even if a person installs

VirtualBox on his/hers *work* PC for himself/herself only. For multiple user enterprise deployments, Kawalek [2012] offers commercial VirtualBox Enterprise licenses for $50 per named user, or $1,000 per processor socket.

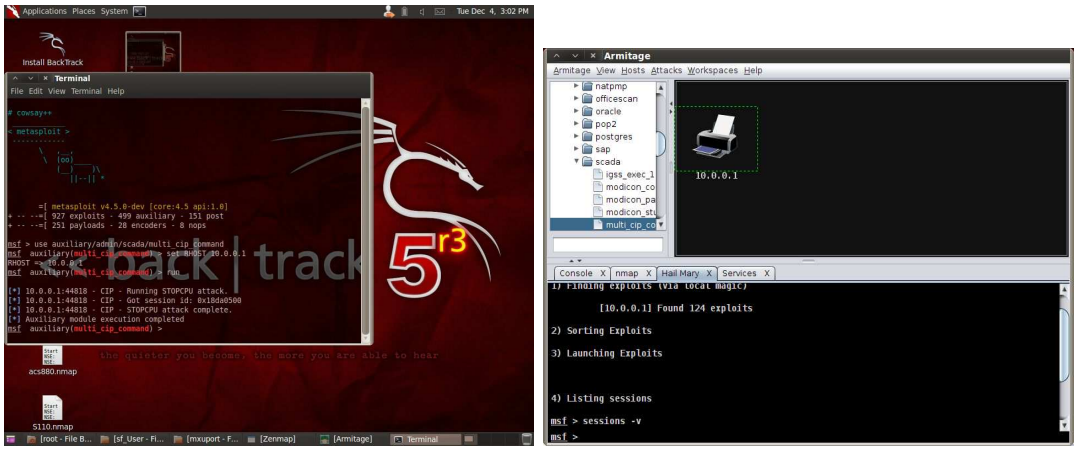
At the time of writing, the latest version 4.2.4, released on October 26, 2012, is available for Windows, Linux, Macintosh, and Oracle Solaris hosts. VirtualBox supports most major operating systems and their versions as guests (virtualized). In this thesis, VirtualBox is used to run BackTrack Linux, and also Windows 7 for the PC tools of AC drives, on a Windows 7 host.

6.3.2 BackTrack Linux

BackTrack is a community-developed Linux distribution for penetration testing and vulnerability assessment. Funded by Offensive Security Ltd., the project is coordinated by Mr. Mati Aharoni (going by the alias "muts"), Offensive Security's lead trainer and developer, with developers mainly from Offensive Security and Tiger Security companies. [BackTrack Linux, 2011a, 2012b, Offensive Security Ltd., 2012c, Tiger Security S.r.l., 2012]

At the time of writing, the latest version of BackTrack Linux is 5 R3 released on August 13, 2012. It is available as 32-bit and 64-bit versions with KDE or GNOME (Figure 20a) graphical desktop environments. BackTrack complies to the GPL by Free Software Foundation. [BackTrack Linux, 2012a, Free Software Foundation, Inc., 2007, Offensive Security Ltd., 2012a]

BackTrack is based on the popular Linux distro *Ubuntu*, which in turn is based on *Debian* used by many high-profile organizations including Siemens, University of Zürich, State of Vermont, and Harvard University. [BackTrack Linux, 2011b, Canonical Ltd., 2013, Software in the Public Interest, Inc., 2012b]



(a) (b)

Figure 20: Screenshots of a BackTrack Linux GNOME GUI session (a), showing the desktop and the console interface (`msfconsole`) to Metasploit Framework (with the `multi_cip_command` auxiliary module in use), and an Armitage session (b) with one AC drive as target.

The next subsections focus on the tools included in the latest BackTrack release (at the time of writing), used in this thesis. Traditionally, exploit tools have been open source and free of charge, but in recent years commercial versions have been developed, as computer security industry has become big business.

6.3.3 Metasploit

Metasploit is software for security assessments. It started as the Metasploit Project in 2003, which resulted in the open source exploit development platform called Metasploit Framework. In 2009, the Metasploit Project was acquired by the Rapid7 company. Nowadays, Metasploit is available in three editions: Community, Express, and Pro. They are all based on the same open source MSF platform, but only the Community Edition is free of charge. The Express and Pro editions are commercial, offering more advanced interfaces and features for penetration testing. Price for Metasploit Express is $5,000, while Pro is individually quoted through a contact with Rapid7. At the time of writing, the latest version of all three Metasploit editions is 4.5.1 released on January 16, 2013. [Andress and Winterfield, 2011, Offensive Security Ltd., 2012b, Rapid7, 2012a,b, 2013]

Metasploit is composed of modules, categorized as *exploits* and *payloads*. Exploits use payloads, otherwise they are called *auxiliary* modules. Payloads are the code to be run remotely. [Offensive Security Ltd., 2012b]

Meta-Interpreter (Meterpreter) is one of the many different types of payloads included in Metasploit. Meterpreter uses a technique called "reflective DLL injection" to load itself into a compromised process running in memory, without using any disk operations or creating any new processes on the host, thus evading detection by conventional methods. [Offensive Security Ltd., 2012b] Examples of typical processes used for the injection are the Windows *Service Host*, `svchost.exe`, and the *Local Security Authority Subsystem Service*, `lsass.exe`, which was used by Stuxnet also for DLL injection [Falliere et al., 2011, p. 14].

6.3.4 Armitage

Armitage (Figure 20b) is a cross-platform, scriptable tool for Metasploit, with a graphical user interface (GUI) that visualizes scanned network targets and recommends exploits against them. It is developed by Raphael Mudge of Strategic Cyber LLC [2013a].

At the time of writing, the latest version of Armitage was released on November 26, 2012, as open source under the Berkeley Software Distribution (BSD) 3-Clause license [Strategic Cyber LLC, 2012]. There is also a commercial version called *Cobalt Strike* available from Strategic Cyber LLC [2013b] for a yearly fee of $2,500 per user after a trial period of 21 days. Designed to emulate APT attacks, Cobalt Strike includes additional features for social engineering and covert command and control (C&C).

Armitage includes an attack called "Hail Mary" for "automatic exploitation". It launches multiple exploits relevant to the target in optimal order. [Strategic Cyber LLC, 2013a]

6.3.5 Nmap—Network Mapper

Nmap ("Network mapper") is a free, cross-platform, and open source tool for network scanning and security auditing. It uses raw IP packets to determine characteristics of large networks or single hosts. First released in 1997 by Gordon "Fyodor" Lyon, Nmap has since become the "de facto standard" tool for network and device scanning. Its latest version (at the time of writing) is 6.01, released in June 22, 2012. [Andress and Winterfield, 2011, Knapp, 2011, Lyon, 2011]

Nmap is able to determine hosts available on the network and their services (ports), operating systems (OS fingerprinting), firewalls, and dozens of other things. Essentially, Nmap is a command-line tool, but there is also a GUI called Zenmap available. It is free, open source, and cross-platform, just like Nmap itself. [Lyon, 2011]

6.3.6 Wireshark

Wireshark is a cross-platform network protocol analyzer supporting hundreds of protocols. It is capable for live capture as well as off-line analysis. [Wireshark Foundation, 2008]

Originally released under GPL as *Ethereal* by Gerald Combs in 1998, the latest version of Wireshark (at the time of writing) is 1.8.4 released on November 28, 2012, under GNU's Not Unix (GNU) GPL version 2 by a team of developers. Under Windows, WinPcap packet capture library is required for live packet capture. [Riverbed Technology, 2012, Sanders, 2007, Wireshark Foundation, 2008, 2012a,b]

6.3.7 The Hacker's Choice-Hydra

THC-Hydra is a very fast on-line password cracker supporting multiple different services, for example file transfer protocol (FTP), HTTP, and Telnet. It supports multiple parallel threads and dictionary files (wordlists) for usernames (logins) and passwords for efficient *brute forcing*. It is essentially a command line tool, but there is also GNU Image Manipulation Program (GIMP) Toolkit (GTK) based GUI available (*HydraGTK*). Distributed as cross-platform open source, the latest version of THC-Hydra (at the time of writing) is 7.4.1 released on December 24, 2012. [Andress and Winterfield, 2011, The Hacker's Choice, 2012a]

First released in August 2000, THC-Hydra is currently maintained by the alias "van Hauser" of The Hacker's Choice (THC), a "non-commercial security group" founded in 1995, and David Maciejak. It is one of the most common password attack tools. [Andress and Winterfield, 2011, The Hacker's Choice, 2008, 2012a,b]

This concludes introduction of the materials used in this thesis. The actual software versions used are listed in Appendix B. Next, the results are presented, starting with the comparison of security related features of the AC drives.

7 Comparison of Security Features of Different AC Drives

The results of the comparison between the AC drives from different manufacturers are presented in this section. They are based on empirical studies and also review of the user manuals. In line with the goal of this thesis, the focus is on security and safety features. Previously, the supporting methods were introduced in Section 5 and the materials in Section 6.

7.1 Commissioning

The AC drives are compared from the application design point-of-view, which basically means configuring the AC drive in such a way that the highest possible security level for that specific device is achieved. The commissioning of an AC drive is of utmost importance for the correct operation of the drive. Usually commissioning includes usage of a PC tool to set the parameters correctly.

The drives from ABB and Rockwell had a "startup wizard" or similar functionality in their control panels for configuring basic parameters such as motor values. That helped the initial commissioning a lot. Consequently, it was possible to run a motor within minutes.

On the other hand, Siemens S110 had a simple control panel compared to the other two drives (visible in Figure 16 on page 58). Probably due to this, it did not offer similar "assistant" functionality. [Siemens AG, 2010]

7.2 Parameter Interfaces

Siemens SINAMICS S110 seems to have two parameter sets: one for the control unit and one for the power module. At first, it was a bit confusing to configure the drive because parameters had to be searched from two different places. Luckily, the STARTER software had wizard-like functionality with dialogs asking values for relevant parameters.

According to Siemens AG [2011b, p. 674], random access memory (RAM) is used to hold modified parameter values until they are manually saved or the drive is powered off. Contents of the RAM are lost without power. The changed parameters can be saved with the "Copy RAM to ROM" function of the STARTER software, or by enabling the parameter p0977 *Save all parameters*.

According to ABB Oy [2012c, p. 24]: "All parameter settings are stored automatically to the permanent memory of the drive." However, it is also possible to manually "force a save" by using the parameter 96.07 *Parameter save*.

ACS880-01 has the parameter 96.02 *Pass code*, but it is described only as "Reserved" in the firmware manual by ABB Oy [2012c, p. 264]. The allowed values are from 0 to 99,999,999.

7.2.1 Access Levels

Rockwell PowerFlex 755 has the parameter 301 *Access Level* with three possible values: Basic, Advanced, and Expert. It defines the amount of parameters visible to the user while browsing them with the PC tool.

Similarly to Rockwell, the Siemens AC drive has different access levels, which are 0 *User-defined*, 1 *Standard*, 2 *Extended*, 3 *Expert*, and 4 *Service*. The highest access level (Service) requires a separate password to be entered into the parameter p3905 *Service parameter* (unsigned 16-bit integer [Siemens AG, 2012b, p. 436]). The current access level is changed by the parameter p0003 *BOP access level* of "the drive object Control Unit". [Siemens AG, 2011b, p. 675]

7.2.2 Reset of Parameters to Factory Defaults

It is possible to restore the default values ("factory defaults") for parameters with all drives. With the Siemens drive, that can be accomplished by the parameter p0970 *Reset drive parameters*, which can also be used to reset specifically the safety parameters if the (*Safety Integrated*) password is set [Siemens AG, 2012b, p. 181]. Otherwise safety parameters are not reset. Similarly to the Siemens drive, ABB ACS880-01 has the parameter 96.06 *Parameter restore*, but it does not reset safety parameters.

Rockwell Automation, Inc. [2012j, p. 66–67] requires the PC tool or the control panel for parameter reset. With the DriveExplorer software, the parameter reset is initiated via: Actions—Non-Volatile Memory...—Load defaults... However, it did not work for the safety module. (The attempt resulted in the mysterious message: "An error occurred during NVS command.") Also attempt to reset the safety parameters with the control panel was unsuccessful (due to "DPI Error: Object State Conflict"). Parameter P7 *Reset Defaults* of the safety module must be used to reset the safety parameters [Rockwell Automation, Inc., 2012a, p. 123]. Which was possible only after the safety configuration was unlocked and P6 *Operating Mode* set to "Program". (More about safety *password* reset later.)

7.3 Functional Safety

As defined in the relevant standards, functional safety was previously introduced in Section 5.4.2. This subsection focuses on safety features and issues included in the AC drives.

7.3.1 Speed Feedback

The feedback types supported by the AC drives compared in this thesis are presented in Table 4. The drives from ABB and Rockwell did not have any encoder inputs as built-in, unlike the Siemens drive. With the additional feedback option modules, the AC drives from ABB and Rockwell support larger amount of different types of encoders than the Siemens drive as standard.

Table 4: Feedback device types supported by the AC drives in their specified configuration, with the specific feedback option modules: ABB FEN-11 Absolute Encoder Interface, Rockwell 20-750-UFB-1 Universal Feedback Module, and Siemens without any *additional* encoder options. (Although, Siemens offers "sensor modules" for cabinets supporting Sin/Cos, EnDat, etc.) [ABB Oy, 2007, Rockwell Automation, Inc., 2011, 2012l, Siemens AG, 2011a, 2012h]

Feedback type	ABB	Rockwell	Siemens
Incremental TTL	x	x	x
Incremental HTL	-	-	x
Incremental Sin/Cos	x	x	-
Absolute SSI	x	x	x
Absolute Endat	x	x	-
Absolute Hiperface	x	x	-

Interestingly, the requirement for external speed feedback for safety functions differs between the manufacturers compared. Rockwell Automation, Inc. [2012b, p. 163] requires an encoder for any safety functions with the *safe speed monitor option module* (20-750-S1). ABB Oy [2012a, p. 23–24] has totally different approach with the FSO-11 *safety functions module*, which uses estimated speed for all safety functions and does not use encoders at all. Siemens AG [2011b, p. 346], with its *safety integrated extended functions*, is in the middle of those two extremes and allows some safety functions to be used without an encoder, while others require it.

Furthermore, there were limitations to which *kind* of encoders could be used with the safety functions, at least depending on the type of the speed feedback option module selected. For example, the Universal Feedback Module for Rockwell AB PowerFlex 755 supports two types of incremental encoders (signals): TTL and Sin/Cos. But as it turned out, only the Sin/Cos type can be used with the safety option (20-750-S1). This observation was confirmed by the *Installation Instructions* manual. However, also the *Dual Incremental Encoder* module (20-750-DENC-1) can be used with the Safe Speed Monitor option, suggesting it should be selected when TTL signals are used for feedback with functional safety. [Rockwell Automation, Inc., 2012b, p. 163]

Measuring the actual speed on the shaft with a tachometer seems like a better solution than using estimated speed, which depends on some kind of software algorithm. Of course, also tachometers have software inside them and they can malfunction. Nevertheless, speed feedback (actual or estimated) is essential for the safety functions described in the next subsection.

7.3.2 Safety Functions

Safety functions implemented in each AC drive are listed in Table 5. According to comparison, it seems that not all of the safety functions advertised by manufacturers are based on the relevant IEC 61800-5-2 standard. At least the names of some functions can not be found from the standard, even though the actual functionality

Table 5: Safety functions with names matching the IEC 61800-5-2 standard implemented in each AC drive: ABB ACS880-01, Rockwell AB PowerFlex 755, and Siemens SINAMICS S110 [ABB Oy, 2012a, Rockwell Automation, Inc., 2011, 2012a, Siemens AG, 2011b]. The names of the safety functions have been conformed according to International Electrotechnical Commission [2007, p. 16–18].

Safety Function	ABB	Rockwell	Siemens
Safe torque off (STO)	x	x	x
Safe stop 1 (SS1)	x	x	x
Safe stop 2 (SS2)	-	x	x
Safe operating stop (SOS)	-	-	x
Safely-limited speed (SLS)	x	x	x
Safe direction (SDI)	-	x	x
Safe brake control (SBC)	x	-	x
Safe speed monitor (SSM)	-	-	x

might be similar. The names of the advertised safety functions without a match in the standard were: safe stop emergency (SSE), safe maximum speed (SMS), safe acceleration monitor (SAM), safe brake ramp (SBR), safe maximum acceleration, and zero speed monitoring. [ABB Oy, 2012a, International Electrotechnical Commission, 2007, Rockwell Automation, Inc., 2011, Siemens AG, 2011b]

Only the safety functions which can be found from the IEC 61800-5-2 standard are listed in Table 5. Otherwise, comparing and interpreting them might be difficult. Although, the standard includes safety functions (covered in Appendix A) which are not implemented at all by the three manufacturers, and those have also been omitted from Table 5.

None of the safety functions applicable for protecting the decanter centrifuge previously listed in Section 5.4.2 are actually implemented in the AC drives. However, substituting safe speed range (SSR) with SLS results to at least the maximum speed being limited, which is more important than limiting the minimum speed. All of the AC drives supported SLS.

7.3.3 Safety Licenses

Two out of the three compared functional safety SLS implementations required an additional hardware module to the drive. Exception was the Siemens S110 which required only a license key.

The safety functions of the SINAMICS S110 drive listed in Table 5 are based on the *extended functions* offered by Siemens, which require a license. (The basic functions, which can be used without a license, are STO, SS1, and SBC [Siemens AG, 2011b, p. 343].) For example, SLS is among the extended functions. Before it can be used, a separate *license key* need to be supplied to the drive. The license key can be first acquired from the Siemens website using the purchased safety license *number*.

Consisting of a maximum of 20 characters, the license key can be supplied to

the drive using the STARTER software. Apparently, the license key is stored on the memory card, which also is a requirement for the extended safety functions. However, according to Siemens AG [2011b, p. 345]: "The associated license key is entered in parameter p9920 in ASCII code." The parameter p9920 (*Licensing, enter license key*) is an array of 100 bytes (octets), each representing one character in the American standard code for information interchange (ASCII) [Siemens AG, 2012b, p. 615]. After the license key is entered to the parameter, it remains visible there and can be read from it at a later time.

Presented by Siemens AG [2011b, p. 706], an example license key is "E1MQ-4BEA". The Siemens *WEB License Manager* (`http://www.siemens.com/automation/license`) is used to generate the license key using the following information: the memory card serial number ("MMC Serial No"), the safety license number ("License No"), and the delivery note ("Dispatch note No"). Thus, the safety license is assigned to the memory card and can not be used elsewhere. [Siemens AG, 2011b, p. 705]

7.3.4 Safely-Limited Speed Configuration

For protection of the decanter, based on its vulnerabilities (described in Section 4), safely-limited speed (SLS) seems to be the most essential safety function of the implementations by the AC drives (Table 5). The descriptions of operation of the SLS safety function by different manufacturers indicate that all implementations stop the drive in overspeed situation [ABB Oy, 2012a, Rockwell Automation, Inc., 2012a, Siemens AG, 2011b]. However, stopping is not required by the IEC 61800-5-2 standard [International Electrotechnical Commission, 2007, p. 17]. An alternative method to stopping would be to limit the speed with the speed controller of the AC drive.

However, while testing the SLS implementation of ACS880-01 it was found out that the drive actually limits the speed. Even though a speed reference higher than the limit was supplied, the drive was running at the limited speed. If the speed exceeded the limit for whatever reasons, the drive tripped (faulted). (The fault was "7A8B FSO_FAULTS_GEN" according to Drive Composer.)

The safety parameters (group 200 *Safety*) of the ACS880-01 are visible in the PC tool and the control panel, but cannot be modified. Only Drive Composer Pro includes the (separate) functionality to set/modify safety configuration.

ACS880-01 has two different, configurable limits for SLS: the speed limit and the trip limit. The speed limit is the value the actual speed will be limited to, despite a speed reference of a higher value is given. The trip limit is the speed which will stop the drive ("safely"). The limits will be enforced after a configurable delay from the time of activation by a digital safety input signal. [ABB Oy, 2012d, p. 124–126]

Configuration of the Siemens *safety integrated* for the S110 AC drive required adjusting settings titled *Monitoring clock cycle* and *Actual value acquisition clock*. It was not a trivial task to set them to correct values, and required many attempts to get them right. Otherwise the drive faulted.

Furthermore, the safety configuration of the S110 drive had to be "copied" be-

tween the control unit and the power module. Like it was possible to configure them both separately.

Grouping of safety parameters of PowerFlex 755 (displayed by DriveExplorer) was very intuitive for commissioning. P21 *Safety Mode* was to be set to one of the many "Lim Speed" options. Then, under the *Limited Speed* group, P52 *Lim Speed Input* set the speed feedback input to be monitored after delay configurable with P53 *LimSpd Mon Delay*. (PowerFlex 755 requires external speed feedback as previously discussed in Section 7.3.1.) The actual limit was configurable by P55 *Safe Speed Limit*. There was no separate trip limit like in ACS880-01. [Rockwell Automation, Inc., 2012a, p. 78]

7.3.5 Password Protection

As previously discussed in Section 5.4.5, the EN ISO 13849-1 standard requires that safety-related parameters are protected from unauthorized modification. However, it leaves a lot of room for interpretation for the actual implementation.

All drives support a safety password. However, the ABB ACS880-01 does not require the password to be *changed* from the default value when safety functions are configured, contrary to the Siemens S110 drive. Regarding this, ABB Oy [2012d, p. 75] states the following: "If necessary, change the password to protect the settings".

For the FSO-11 safety option module by ABB Oy [2012d, p. 73], the default password is 12345678. It can be changed to any *number* with 4–8 digits. So, the password can consist of only numbers with maximum length of 8. The reason for such a small maximum length limit remained unknown, because a parameter for the safety password was not found in the drive parameter lists, nor mentioned in the manual. Unfortunately, it was not possible to change the password from the default due to ABB's Drive Composer Pro crashing each time the "Change password" button was pressed.

Rockwell has a whole subgroup of parameters under the title "Security" for the Safe Speed Monitor option. It implies that they are taking safety seriously, by dedicating security options for protection of safety configuration. However, Rockwell does not require a safety password to be set. It is optional and up to the user to decide whether he/she wants to "lock" the safety configuration.

The default safety password for the Siemens S110 is 0 (zero). The parameter for the password has a data type of 32-bit unsigned integer (corresponding to possible values from 0 to 4,294,967,295). However, STARTER did not allow passwords with more than 8 numbers. [Siemens AG, 2011b, 2012b]

According to Siemens AG [2011b, p. 350]: "The Safety password is retained on the memory card and in the STARTER project." The password is required to restore safety settings to the factory defaults. However, it is possible to download a new project into the drive *without any* password after restoring *all* settings to factory defaults and recommissioning the drive with a new drive data set (DDS).

7.3.6 Safety Password Reset

All three manufacturers offer the user possibility to reset a forgotten password. For this, Rockwell Automation, Inc. [2012a, p. 122] requires contact to their technical support with "the Security Code value and the serial number of the safety option." The Security Code can be read from the parameter 18 (P18) of the safety module. The 8-digit serial number is also available remotely with DriveExplorer and on the web interface (if enabled). Then, Rockwell's technical support provides a "Vendor Password" (parameter 19) which initiates reset for the safety password. The data type of the vendor password parameter is unsigned 16-bit integer (0–65,535).

ABB and Siemens allow reset of the safety password without contacting them. A "factory reset" will clear the password for both drives. Factory settings can be restored with a physical button on the FSO-11 safety module by ABB Oy [2012a, p. 143] or remotely for the whole S110 drive by Siemens AG [2011b, p. 350].

A bit alarming from the security point of view is that Siemens expresses that they are able to determine the safety password forgotten by the user. For this, Siemens AG [2011b, p. 350] requires the "complete drive project" which refers to the configuration created and downloaded to the drive with the STARTER tool for example. (By default installation of the STARTER software on Windows 7, the project files are located in the folder `C:\Program Files\SIEMENS\Step7\s7proj` indicating they are similar with the Siemens SIMATIC STEP 7 software used to program PLCs [Siemens AG, 2012d].)

Even more alarming is the fact that Siemens AG [2011b, p. 350] provides instructions how to change safety settings without knowing the password. The three-step procedure starts with resetting the whole drive to factory defaults, after which it is possible to recommission first the drive and finally the safety parameters.

7.4 PC Tools

Generally, the PC tools for the three AC drives tested allow *total* configuration remotely. For Rockwell and Siemens, remotely means by Ethernet—For ABB, by USB, even though Ethernet access should be available according to ABB Oy [2012b, p. 14–16], possibly in the future. However, not one of the PC tools tested provided user access control and authentication. Which makes sense if the features are not supported by the network devices, the AC drives.

In the Siemens STARTER software, there is a functionality called *Know-how manager* which allows a login (a username) and a password to be used with the project. The minimum length for the password is five characters. According to Siemens AG [2012c], know-how protection is used protect "intellectual property" against "unauthorized use or reproduction". When activated for a "drive unit", the parameters can not "be read or written". Optional "copy protection" feature links the project with the serial number of the memory card, preventing the project from being used with other memory cards. Additionally, the know-how protection can be made permanent ("absolute know-how protection") so that it can not be removed. It is also possible to allow certain parameters to be read-only while the rest are

protected from reads and writes. Know-how protection requires "SINAMICS V4.5 or higher".

The DriveExplorer software from Rockwell offers multiple "wizards" to ease drive configuration. Unfortunately, all of them did not work. One of the working ones was *DPI/DSI Tech Support Wizard* (revision 3.3.7) which gets all relevant parameter values and version details from the AC drive into a single text file with ASCII encoding.

7.4.1 Communication Protocols

According to a Wireshark capture, the Siemens STARTER software communicates with the S110 AC drive using T.125 (*Multipoint communication service* by International Telecommunication Union [1998]) and ISO-TSAP (defined in request for comments (RFC) 1006 by Rose and Cass [1987]) [Langner Communications GmbH, 2011] protocols. According to Siemens AG [2011b, p. 593], the "S7 protocol" is used with STARTER in on-line mode for acyclic parameter reads and writes.

Rockwell's DriveExplorer communicated with the PowerFlex 755 drive using EtherNet/IP objects. According to Rockwell Automation, Inc. [2012g, p. 123–124], PowerFlex 750-Series AC drives have (limited) compatibility with the following EtherNet/IP explicit messaging class codes for parameter reads/writes: "DPI Parameter Object 0x93" and "Host DPI Parameter Object 0x9F".

ABB's Drive Composer Pro could not communicate over Ethernet, but used USB instead. Thus, it was not possible to monitor the traffic and the used protocols with Wireshark, which does not support USB capture under Windows OS [Wireshark Wiki, 2011].

7.4.2 Communication Libraries

The Siemens software package included many separate programs in addition to the actual STARTER tool, including *Automation License Manager*, and *SIMATIC Industrial Ethernet (ISO)* and *PROFINET IO RT-Protocol V2.0* network "drivers" automatically attached to the Windows LAN connection. An alarming discovery was the file `s7otbxdx.dll` under `C:\Windows\System32` (on 32-bit Windows 7). That is exactly the same filename which Stuxnet reportedly replaced to attack the Siemens PLC (described in Section 3.1.4) [Falliere et al., 2011, p. 36]. Digging through the properties of the file with Windows (file) Explorer, it described itself as "STEP 7 Block Administration" for "SIMATIC Device Operating System®" by "SIEMENS AG 2006-2011". The date of last modification was November 4, 2011. It is signed by "SIEMENS AG" with the MD5 "digest algorithm" and the Rivest-Shamir-Adleman (RSA) "digest encryption algorithm" issued by VeriSign. However, the signature is missing information about e-mail address and signing time, hence its validity period could not be verified by Windows.

The PC tools from the other two manufacturers had similar files related to communication between the PC and the AC drive: `CComm.dll` ("Generic Communication layer for DriveExplorer") and `EnetComm.dll` from Rockwell, and `PhloemComm.dll`

from ABB. Contrary to the Siemens DLL, the ABB file has signature with the signing time (May 31, 2012), thus Windows reports it as "OK". The digital signature is issued to "ABB Oy" by "VeriSign Class 3 Code Signing 2010 CA". The files from Rockwell were not signed at all.

7.5 Ethernet

This subsection concentrates on the security features specific to the Ethernet communication bus. Ethernet was previously discussed in general in Section 5.2.

The AC drive models from Siemens and Rockwell have Ethernet-based fieldbus built-in. ABB's ACS880-01 has it only as an additional option module.

7.5.1 Internet Protocol Address Configuration

The ABB FENA-11 Ethernet fieldbus adapter (FBA) supports static and dynamic IP address configurations. If the drive is previously configured to use a static IP address, setting it to dynamically assigned through a dynamic host configuration protocol (DHCP) server clears the static IP address. This makes it hard to figure the once assigned IP address for the drive, in case the configuration is changed from static to dynamic by accident or maliciously.

To complicate things even further, the parameters responsible for the IP address are named generically as "FBA Par4", "FBA Par5", etc. Unless the user has memorized the meaning of the parameters, the user's manual for the FENA adapter is required to configure the drive properly.

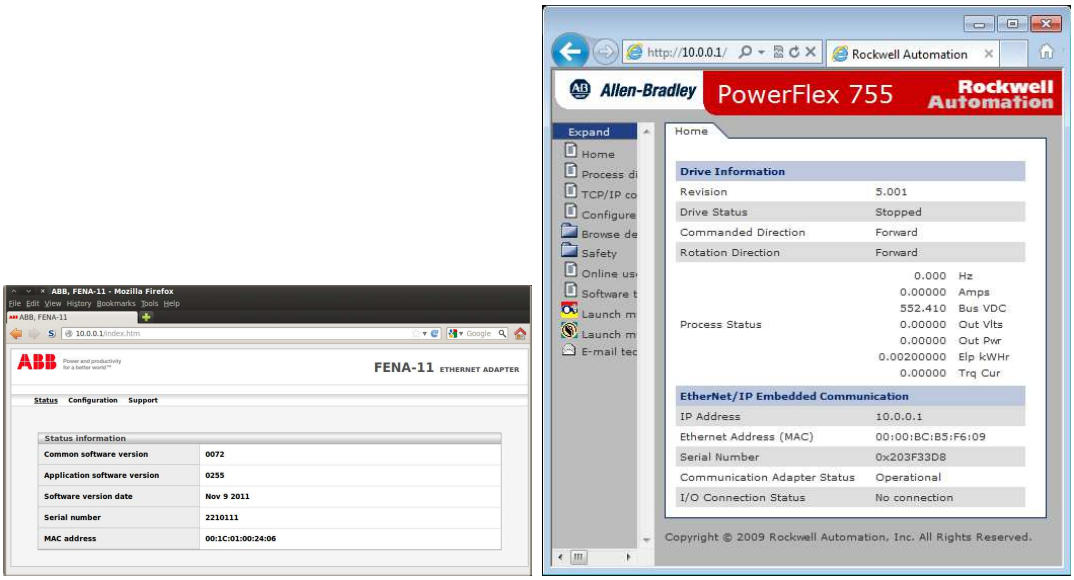
An IP address for the SINAMICS S110 drive is assigned by Primary Setup Tool by Siemens AG [2012g] available directly on their website free of charge. Without it, the drive was not available to be connected by the STARTER software through Ethernet (PROFINET) for further configuration.

PowerFlex 755 supports three sources for the IP address configuration (parameter 37 *Net Addr Src*): Physical switches, parameters (38–41 *IP Addr Cfg 1–4*), and the bootstrap protocol (BOOTP). It was possible to "hide" the Rockwell PowerFlex 755 AC drive from the network by configuring the IP address to 0.0.0.0 and rebooting the drive. To restore Ethernet communications, it was required to use direct serial connection (through the USB-DPI adapter) or the control panel (locally) to revert the IP address to a valid one. Both ways require physical access (unless the USB-DPI adapter (or similar) is used over a remote connection).

7.5.2 Web Interfaces

ABB and Rockwell have web interfaces, i.e. port 80 for hypertext transfer protocol (HTTP), open by default, but Siemens did not. The front web pages are presented in Figure 21. No authentication was required to access the web interfaces.

For Rockwell PowerFlex 755, the web interface can be enabled with the parameter 52 *Web Enable* of EtherNet/IP Embedded and by rebooting the drive. However, even though it was *not* enabled (the default mode), the drive responded to a basic



(a) (b)

Figure 21: Front pages of the web interfaces for the ABB ACS880-01 (a) and Rockwell AB PowerFlex 755 (b) AC drives.

HTTP request (GET method) with the 404 (*Not Found*) error message. Evidently, there must be a HTTP daemon (a server) running, although totally unnecessarily.

Through the web interface of PowerFlex 755, it is possible to modify safety configuration, although it requires the safety password *if* one is set (which is optional for the Rockwell drive as previously described in Section 7.3.5). ACS880-01 allows configuration modifications only to the Ethernet-based fieldbus settings through the web interface.

For ABB ACS880-01, it was not possible to disable the web interface separately. However, it was possible to disable the fieldbus adapter (by the parameter 50.01 *FBA enable*), which prevents all Ethernet communications.

7.5.3 Parameter Writes and Memory Wear

A warning about potential "equipment damage" related to parameter writes is given by Rockwell Automation, Inc. [2012g, p. 123]: Frequent "Explicit Messages" with parameter writes to "Non-Volatile Storage (NVS)" will cause the NVS to "quickly exceed its life cycle and cause the drive to malfunction." The warning is repeated on many occurrences throughout the user manual for the embedded EtherNet/IP adapter. A mechanism called *Datalink*, which writes to volatile memory, should be used for frequent parameter value changes [Rockwell Automation, Inc., 2012g, p. 109–110].

It is also explicitly expressed that the NVS is electronically erasable programmable read-only memory (EEPROM) [Rockwell Automation, Inc., 2012g, p. 132]. In practice, it is most likely cheaper Flash memory.

However, a similar kind of warning about premature failure of memory is not

presented in the user's manual for the FENA Ethernet adapter by ABB Oy [2011b, p. 141, 215], even though it supports explicit messaging through EtherNet/IP. It is noted though, that updates to parameters specific to the fieldbus configuration are taken into effect only after a certain refresh procedure is made.

According to Siemens AG [2011b, p. 596], parameter writes using the PROFIdrive profile and PROFIBUS (DPV1) requests are done to RAM. The changes can be saved to non-volatile memory using the parameter p0977. Notes or warnings about premature memory wear are not given in the manual.

7.5.4 Vulnerability to Common Exploits

The Hail Mary attack of Armitage was executed on each of the three AC drives. Despite trying 21 exploits on Siemens and 124 exploits on ABB and Rockwell, the attacks did not succeed. The result was "No active sessions" with all three attempts.

In addition, exploit against the common industrial protocol of EtherNet/IP (described in Section 5.3.3) was unsuccessful against the AC drives using the protocol: ACS880-01 and PowerFlex 755. All attacks offered by the Metasploit module `multi_cip_command` did not affect the drives in any noticeable way. Especially communication was not disconnected. That is particularly interesting for PowerFlex 755 by Rockwell, which was the vendor affected in the original disclosure.

The Siemens S110 drive has FTP and Telnet ports (23 and 22, respectively) open. Both of them required a correct username and a password. Brief attempt with THC-Hydra (introduced in Section 6.3.7) and some wordlists found from the Internet was not successful for gaining access to those services.

7.6 Firmware Updates

Siemens did not offer firmware updates for the SINAMICS S110 directly through Internet. Instead, they are offering multimedia cards (MMCs) including the firmware [Siemens AG, 2013]. This efficiently prevents contents and protection of the firmware to be analyzed, at least by random hackers, unless social engineering attack against *wetware* (Siemens support personnel) is conducted successfully to achieve the firmware. Firmware images, which are freely available on-line for download, can be analyzed and detailed information gained with relatively ease, as has been demonstrated by Gervais [2012, p. 61–62] among others.

While the S110 firmware image was not freely available for download, once acquired it was extremely easy to load it to the drive using the MMC. First, the previous contents on the MMC were erased, then the files from the compressed firmware image package were copied to the root folder of the MMC. Siemens S110 drive automatically starts update process if it detects that there is a new firmware on the MMC. However, this offers possibility for a malware to replace the contents of a MMC connected to an infected computer to propagate to and infect the AC drive also.

Rockwell offers firmware updates for their AB PowerFlex drives freely for download without registration [Rockwell Automation, Inc., 2012c]. According to Rock-

well Automation, Inc. [2012i, p. 4], firmware "flashing" can be performed using the 1203-USB converter or the 1203-SSS *smart self-powered serial* converter. However, the *PowerFlex 755 Drive Embedded EtherNet/IP Adapter* user manual states that the adapter firmware, contained in the drive firmware, can be updated also "over the network" [Rockwell Automation, Inc., 2012g, p. 42]. Indeed, DriveExplorer was successfully used to update the firmware using the function "Flash Upgrade" over the Ethernet. Alas, without any authentication, so anyone in the same network as the PowerFlex 755 drive can change how the drive functions by reprogramming the firmware.

ABB's approach to ACS880-01 firmware updates is similar to Siemens in the sense that they are offering memory units instead of loading packages to customers [ABB Ltd, 2010]. However, ABB's memory units are not compatible with conventional PC memory card readers, making firmware reverse engineering a bit harder.

7.7 Miscellaneous Features

This subsection presents miscellaneous features related to security discovered during the comparison of the AC drives, but not discussed in the earlier subsections.

7.7.1 Factory Seal

Even though security in the supply chain for AC drives is not in the scope of this thesis (as expressed in Section 1), it was noted that Rockwell supplied their components in packages with stickers saying "FACTORY SEAL" on them. Also Siemens had placed a sticker stating "ORIGINAL PACKING" to a strategical location on the package for the control unit.

These kinds of "factory seals" provide some sort of "proof" that devices have not been tampered in the supply chain after departing the manufacturer. Of course, basic stickers, which do not have features such as holograms, can be easily counterfeited and replaced.

7.7.2 Critical Speeds

Critical speeds, meaning rotating frequencies resulting to resonance of decanter centrifuges, were previously discussed in Section 4.2.4. AC drives have built-in features to combat them.

ACS880-01 has a function called *critical speeds* (or frequencies) for avoiding specific motor speed ranges due to mechanical resonance problems. It works for both rpm and Hz type speed references. Three speed ranges can be set up through the parameters (with values limited to ±30,000 rpm), causing the drive to "jump over" them. [ABB Oy, 2012c, p. 36–37, 153]

S110 has a similar function called *suppression bandwidths* which can be used to avoid resonance frequencies. A total of four "skip" speeds can be set (each between 0 and 210,000 rpm) where steady-state operation is not allowed. [Siemens AG, 2011b, p. 291–292]

PowerFlex 755 did not have a corresponding function. However, similarly to the other two drives, it also had limits for maximum and minimum speeds, acceleration, and deceleration. [Rockwell Automation, Inc., 2012j]

7.7.3 Write Masks

The Rockwell PowerFlex 755 AC drive has masks, which can be used to prevent "commands" reaching the drive. In the "parameter tree" displayed by the DriveExplorer software, the masks can be found under PowerFlex 755—Communication—Security. Parameter 888 *Write Mask Cfg* is used to disable parameter *write* access for "DPI ports". Those ports are used for different "devices" inside or connected to the PowerFlex 755 drive, including the control panel (HIM), EtherNet/IP Embedded, and Safe Speed Monitor. [Rockwell Automation, Inc., 2012j, p. 59–61] Consequently, the write mask can be used to disable parameter modifications from the fieldbus while allowing parameter reads for remote monitoring purposes.

Bit 13 of P888 was unset to disable writes from Embedded EtherNet/IP, and the drive was powered off and back on to make the change effective. Connected through Ethernet network, DriveExplorer could read parameters but not modify their values. Evidently, the PC tool detects the write mask because the views for individual parameters were different than without the protection enabled. (They were missing the "OK" and "Apply" buttons.)

The control panel could be used to set the bit 13 back, restoring write access to fieldbus after power cycling the drive. DriveExplorer required also reconnection.

This concludes the description of the comparison and the observations made during it. In the next section, overall results of the thesis are presented, starting with summary of the results of this comparison.

8 Results

In this section, the results of the thesis are presented to the reader. Also the research questions introduced in Section 1 are answered.

8.1 AC Drive Security Related Feature Comparison Summary

Comparison of different AC drives was described in the previous section. A summary of the comparison of the security features of the AC drives is presented in Table 6.

It must be noted that these devices are not intended for public networks, and never have been. It's been up to the upper controllers (e.g. PLCs) to handle network security. The traditional job of an IED, such as an AC drive, is to respond to the master's requests as fast as possible, without questioning the authenticity of the request.

Table 6: Overall summary of the comparison of security related features of the three AC drives: ABB ACS880-01, Rockwell AB PowerFlex (PF) 755, and Siemens SINAMICS S110. All port numbers are for TCP unless stated otherwise.

Security feature	ABB ACS880-01	Rockwell PF 755	Siemens S110
Safety password (PW) strength	8-digit integer	32-bit unsigned integer	8-digit integer
Default safety PW	12345678	- (*no password*)	0
Safety password reset by ...	Physical button	Vendor password	PC tool or parameter p0970
Web server enabled by default (port 80 open)	Yes	Yes	- (no web interface at all)
Other open ports	44818 EtherNet/IP	44818 EtherNet/IP	21 FTP, 23 Telnet, 102 ISO-TSAP, 161/UDP SNMP, 3841, 3843
PC tool over Ethernet	No	Yes	Yes
Protocols used by the PC tool	Unknown (USB)	44818 EtherNet/IP	102 ISO-TSAP/T.125
Communication libraries signed	Yes	No	Yes, but signature invalid
Distribution of firmware updates	Customer service	Freely downloadable	Customer service
Firmware update process by a ...	Memory unit (ZMU)	PC tool	Memory card (MMC)
Parameter writes automatically saved	Unknown	Yes/no, depends on the method	No
Other features	Critical speeds	Write masks	Know-how protection

8.2 Recommendations for Securing the Decanter Application

This subsection presents recommendations for securing the decanter centrifuge, connected to an industrial Ethernet network, against cyber sabotage by an advanced, Stuxnet-like threat. Essentially, the recommendations can be seen as mitigation strategies for vulnerabilities of AC drives. However, many security defects are related to the fieldbus architecture, and the recommendations are not specific to certain AC drives, but apply to similar automation installations in general.

Assuming a PLC is included with the decanter, it can not function as an adequate "firewall". Therefore, the following recommendations are applicable as compensating measures for the inherently poor security status of ICS, based on the current situation.

8.2.1 Protecting Decanter Centrifuge Vulnerabilities

Vulnerabilities related to decanter centrifuges were previously discussed in Section 4. AC drives offer many functions to protect the equipment so that it can operate safely. The most obvious vulnerability related to critical speeds can be protected by methods discussed later in Section 8.3. This subsection concentrates on the other vulnerabilities.

The back drive should be configured with strict torque limits to prevent the delicate gearbox wearing out too quickly. The main drive should monitor the temperature of the main motor to inhibit start if the motor is not cool enough, and also stop the motor if it gets too hot during acceleration of the bowl.

Maximum current limitation and stall protection are also important for each motor. Acceleration and deceleration times should be set for the main drive so that the belts will not slip.

8.2.2 Air-gap

Stuxnet was able to cross air-gaps on portable media, demonstrating that cyberwar does not require Internet for a successful attack. However, disconnecting from the Internet greatly complicates the effort needed by an attacker.

The decanter centrifuge should not be directly accessible on the Internet (with a public IP address). If remote monitoring through public Internet is needed, at minimum, it should be routed through an encrypted virtual private network (VPN) connection to a server/router at the decanter site.

Even if an AC drive supported IPv6, it should have a private IP address only. This is important especially in the future.

8.2.3 Indications

Stuxnet supplied false data to monitors. Consequently, the operators were not aware that the gas centrifuges were not running correctly, as previously described Section 3.

Therefore, if an AC drive is limiting the speed for whatever reasons, indication about that might not reach the control room, the appropriate systems or persons. With this in mind, the value for the speed limit should be set so that the decanter centrifuge can withstand it without being damaged for extended periods of time.

Change in speed affects quality of materials (the cake and the centrate) output by a decanter centrifuge. Ultimately, production quality control can reveal a compromised control system. Extreme form of this is production halt, for example in case of totally isolated SIS which automatically shutdowns the decanter centrifuge in overspeed situation.

As previously discussed in Section 5.2.3, network/fieldbus traffic should be monitored with an application monitor or an industrial protocol monitor. For example, an attempt to disable maximum speed limits of an AC drive by writing to relevant parameters through fieldbus (similarly to Stuxnet discussed in Section 3.4.1) can be detected this way.

8.2.4 The Human Factor

Decanter plant operators and other technical staff with access to confidential information such as passwords should be trained against social engineering attacks (introduced in Section 2.2.2). Also, the staff should be trained to use strong personal passwords efficiently, for example by using certain patterns. There are free and commercial solutions (applications) for efficient personal password management.

It is also important to protect a session from trespassers, by locking the console when "away from keyboard" (e.g. on a break). Otherwise, someone could act with the operator's credentials, making tracing more difficult or impossible depending on physical security measures such as surveillance cameras. There are applications which utilize basic "web cameras" (webcams) for facial recognition and motion detection, automatically locking the workstation while the user is away.

8.2.5 Application Whitelisting

Previous incidents have proven that digital certificates can not be trusted because they can be stolen or the issuing authorities can be compromised (as previously described in Section 2.2.4). Thus, even digitally signed programs should be prevented from being executed unless specifically allowed.

Application whitelisting introduced in Section 5.2.3 is well suited for ICS and SCADA environments. It should be used, preferably, on all devices within the network, but most importantly, on computers used to communicate with the decanter centrifuge.

During the making of this thesis, the PC tools for the AC drives were run inside a Windows 7 virtual machine (VM). Software and related USB devices from all three manufacturers worked well under VirtualBox. Even though in this case also the VirtualBox host was Windows 7, it should not make a difference if the host is Linux, for example. This means that the computer used to configure the decanter centrifuge can have Linux as main OS for security purposes, and the software for AC drives and other devices can be run inside VirtualBox VMs.

However, depending on the technical solution, an AWL product might be ineffective against malware which "injects" itself into the memory used by legitimate programs. Stuxnet did it and also the Meterpreter shell of Metasploit does it. Therefore, it is imperative that the AWL solution is comprehensive and not limited to filenames for example (like the "Run only allowed Windows applications" policy by Microsoft [2013b]).

Nevertheless, the "whitelisted" (allowed) applications might be exploitable. There are free tools available to strengthen the execution environment security for a single application, for example the Enhanced Mitigation Experience Toolkit by Microsoft [2013a].

8.3 Overspeed Protection

Analysis of the Stuxnet case (Section 3) revealed that overspeed protection is crucial for protecting centrifuges against cyber sabotage. Different ways to implement overspeed protection with decanter centrifuges are discussed next.

8.3.1 Speed Limit Parameters of AC Drives

Firstly, all AC drives have some sort of speed limits, which are configurable through their parameter interfaces. The problem with those in fieldbus environments is that the parameter interface is open to modifications without authentication (usernames, passwords, logging, etc.). Some drives incorporate parameter write masks (previously detailed in Section 7.7.3) which can be used to prevent parameter modifications from the fieldbus, thus offering protection for the speed limits from remote tampering.

However, parameter write masks do not protect in case the actual speed of rotation of the centrifuge somehow exceeds the safe operating range for whatever reason (for example due to misconfiguration, software malfunction, sensor defect, etc.). Functional safety provides additional protection, regardless of the root cause for the overspeed situation.

Furthermore, a safety system for centrifuge overspeed protection is mandatory with AC drives according to European standards (as previously described in Section 5.4.4). The SLS safety function fulfills the requirement.

8.3.2 Functional Safety and Safely-Limited Speed

The standardized *safely-limited speed* safety function is well-suited for preventing the decanter centrifuge from running too fast to be safe. An AC drive equipped with the SLS functionality limits the speed according to the safety configuration despite a higher speed is requested (through the speed reference from the fieldbus, for example). And if the speed exceeds the safety limit for whatever reasons, the drive engages a safe stop procedure which transitions the decanter centrifuge to a torque free state, ultimately coasting to standstill.

Usually, decanters operate at speeds which do not prohibit the use of speed feedback devices. Therefore, whether or not the AC drive requires feedback for the

SLS safety function is not relevant. However, it could be argued that measuring the actual speed of rotation directly from the shaft is better than calculating (estimating) it with some algorithms. On the other hand, an encoder is one additional component which can break. However, AC drives have monitoring and protection features also for encoder fault situations.

Functional safety is configured with the AC drive commissioning tools and protected with a password. Therefore, it is not a totally independent and isolated safety system. Also, the safety passwords are generally weak due to limitations placed by AC drives themselves (as presented in Section 7.3.5). For better protection against remote tampering, traditional, completely isolated safety instrumented systems offer safety without monitoring possibilities for SCADA applications for example.

8.3.3 Completely Isolated Safety Instrumented System

A SIS for decanter overspeed protection should be able to monitor the speed of rotation and stop the machinery if safe operating range is exceeded. With induction motors and basic scalar control for example, the speed can be calculated from the frequency supplied to the motor. There are electrical devices available for that purpose. Furthermore, in case the frequency exceeds some specified value, the main contactor of the decanter should be opened (de-energized), shutting down the AC drives and stopping the centrifuge. The control units can be powered by a separate +24 V supply so that they can still communicate with rest of the plant, and indicate that the decanter centrifuge has been shutdown.

Being totally isolated in principle, the safety system could not indicate the reason for the shutdown through fieldbus. However, some digital outputs could be connected to the basic I/O inputs of AC drives or a PLC, which could forward the status to monitors.

8.3.4 Cybersecurity Checklist for AC Drives in Decanters

A checklist for achieving AC drive configuration with maximum security using SLS is presented in Appendix C (on page 118). It can also serve as a template for vendor-specific guidelines.

The checklist consists of multiple steps designed to be followed in the order from top to bottom. By all means, the individual steps are not trivial. Each step on the checklist is practically a mini-project in itself, with multiple internal steps.

Unfortunately, the detailed contents and actions related to each step on the checklist can not be presented in the context of this thesis, because of the extent of the related issues. Further information can be found, for example, from the source materials of this thesis (the listing of references starting from page 93).

Not specific to any real AC drive product on the market, the checklist gives guidelines for an imagined, generalized industrial AC drive. Some of the features may or may not be available in the AC drive actually being commissioned and configured. Thus, it is a good idea for real implementations to modify the checklist according to the specific components (AC drives, motors, option modules, etc.) used.

The checklist can also serve as an addendum for a larger security program covering a wider range of equipment, possibly the control system of a whole industrial plant. Recommendations and templates for ICS security programs have previously been presented for example by ABB [2010b], Stouffer et al. [2011], Huhtinen [2011], and European Network and Information Security Agency [2011].

8.4 Recommendations for Improvement of Security of AC Drives

This subsection describes how security of AC drives could be improved by product development and engineering. Therefore, the discussion in this subsection is aimed towards manufacturers, not customers of AC drives. During the making of this thesis, it became evident that AC drives have a lot of potential for improving their security features. Therefore, these recommendations are for better future. Some of them are the same as previously described for field devices in general in Section 5.3.2.

8.4.1 Ethernet Vulnerabilities of AC Drives

The drives were not vulnerable to some common exploits as previously described in Section 7.5.4. However, there were several issues which can be seen as vulnerabilities.

The web servers in the AC drives which had them could not be disabled. Thus, the TCP port 80 was constantly open even though it was not used. An attacker might find a way to exploit the web server to gain unlimited access to the drive. On the other hand, it was possible to modify only a handful of parameters by default through the web interface.

More serious consequences can result from the unlimited, anonymous access to *all* parameters through the Ethernet in the AC drives which supported it. A person with the software for the drive can generally change everything. The software might use some internal, secret passwords to prevent third party applications using the same communication protocols, but it can be regarded as a very weak protection as the official programs are easily available. It is also possible to analyze the communication protocols for any "secret" codes.

The issues presented above are probably the result of conscious choices made by the manufacturers. As such, they are not flaws in implementation or design, but in specification instead. However, specifications are usually based on customer demands, so in the end customers decide which issues need to change. The author's personal opinion is presented next.

8.4.2 Safety Password Complexity

Safety passwords should be as complex as possible (maximum entropy). If the safety password is supplied through a parameter, the data type should allow characters in addition to numbers.

This can be accomplished with the solution Siemens is using for supplying a safety license key to the drive: a parameter array with 100 bytes (8 bits in each

cell), allowing 255 different values for each byte, so the full extended ASCII set can be used for the key, or the string. Extended ASCII includes all alphabets, numbers, accent characters (e.g. å, ä, and ö), and special characters such as !, /, #, etc. A password with that complexity and a maximum length of 100 characters can be considered very strong, at least if password policy for the minimum length is adequate. This makes brute force attacks practically futile.

Recommendation: Implement an alphanumeric safety password policy with *minimum* length of 8.

8.4.3 Parameter Modification Protection

It should be possible to protect parameters from modification (writes) and perhaps from reads also, at least in some case with some particular parameters which can reveal sensitive information such as version numbers, which could be exploited in an attack. This could be implemented by making just one parameter always writable: some kind of a password parameter, which could be used to disable the write protection of other parameters *temporarily*. The parameter for the write protection password should be equally strong as the safety password described in the previous subsection. It should be encrypted during transmission due to potential "sniffing".

With advanced AC drives capable of running custom user applications (for example by ABB Ltd [2012]), extending a similar kind of modification protection for application programming should be considered. Example could be taken from some PLCs with a *physical* switch for preventing modifications to the PLC program while allowing certain variables to be used. Also some memory cards have a switch to protect the contents from modification. [ICS-CERT, 2012a] However, it is evident that requiring physical access and presence for each update is not feasible in all industrial facilities.

Recommendation: Implement protection against unauthorized parameter modifications (at least from the fieldbus).

8.4.4 Access Control for Tools

All AC drives offer some kinds of service interfaces which are utilized by PC tools used for commissioning and configuring the drives. Being normal Windows applications, there is no reason why they could not have a login/password prompts before allowing total access to an AC drive. Other protocols such as Telnet and FTP offer this kind of minimum access control method.

Recommendation: Implement login/password access control to the PC tool interface.

8.4.5 Configuration of Network Services

AC drives should offer the customer and end-users possibility to disable network services such as HTTP servers. Every running network service can be a security risk. They are not required in all applications.

According to reduction strategies presented by Langner [2011a, p. 48], everything that is not needed should be removed or disabled. The less complexity the better.

Recommendation: Make all network services configurable so that they can be disabled by the user.

8.4.6 Access Control for Web Services

Web (HTTP) services are the most accessible of network services, because practically all computers (and nowadays also phones) have a web browser. It is very inconvenient if just some random "web surfer" can change configuration settings of an AC drive connected to the same network. For this reason, even devices such as webcams and WLAN access points intended for home networks and private use have login/password protection in their web interfaces. There is no reason why an industrial device would not have the same minimum protection.

For example, most modern network devices have a requirement for both the username and the password. But even just the password is better than nothing.

Recommendation: Implement login/password access control for the web service.

8.4.7 Firmware Updates

It needs to be seriously considered, how to organize distribution of firmware updates through the Internet. At stake, there is the knowledge of the internal structure of the firmware, on the other hand user support.

If the firmware updates are to be distributed freely over the Internet, very strong encryption algorithms should be used to prevent reverse-engineering. However, the resulting need for decryption performance at the AC drive end might be too much for the relatively low-performance processors used in AC drives.

From the security point of view, a better strategy for firmware update distribution is through customer service or something similar, so that the recipients can be tracked and the packages be restricted only to certain hardware, using serial numbers for example.

Also, the way in which the firmware update can be performed should be secure. For example, leaving the AC drive open to any remote firmware uploads without authentication is dangerous. (According to Langner [2011a, p. 129], the related vulnerability was dubbed *Boreas* by DHS in 2007.)

Recommendation: Restrict firmware updates to only certain reliably identifiable and traceable transmissions from authorized users/stations.

8.4.8 Logging of Security Related Events

Current AC drives collect logs for faults and other events generated during operation. Security related information, such as failed password attempts, could be included in the logs also. Logging is important part of detecting cyber attacks.

Recommendation: Include security related events in the logs.

8.5 Conclusion

It is possible to protect decanter centrifuges against cyber sabotage using special features of AC drives. However, being remotely accessible devices, AC drives can never offer the same level of security as compared to totally isolated safety systems. For ultimate protection of critical applications, isolated, single-function SIS for overspeed protection should be implemented.

However, multiple layers of defense need to be penetrated by the attacker/malware before reaching the AC drive, including possible physical security measures, network security such as firewalls, possibly compromising a PLC or other "master" control device, and finally modifying the fieldbus traffic to alter operation of the AC drive. Consequently, protection against cyber sabotage is never solely up to the AC drive.

8.5.1 Significance of the Results

The meaning of these results is that a decanter centrifuge can operate in critical facilities and applications, such as uranium ore dewatering, without a significant concern for it being physically damaged by a cyber threat. Thus, the risk level related to cybersecurity is reduced.

However, it does not mean that networked decanters can be left totally without attention from cybersecurity point of view. As discussed earlier, there is always need and even demand to constantly monitor the network for unauthorized actions and potential malware.

8.5.2 Reliability of the Results

The results of this thesis are mainly based on publicly available literature and empirical studies made with three different AC drives. IT security is well-established discipline evolved over the period of the last couple of decades. However, it is constantly evolving. ICS security has been under scrutiny for a relatively short period of time. Furthermore, methods combining safety with security seem to be only emerging.

The security and safety guidelines presented as the results of this thesis are based on current theories and principles. The main source literature regarding security is post-Stuxnet, meaning it has been published after the year 2010. All other literature is also mainly from the 21st century.

However, the *Decanter Centrifuge Handbook* is over 10 years old. Technology has advanced since then, especially related to remote control and monitoring (PLCs, fieldbuses, etc.). And has probably become more widespread. Therefore, the solutions used today might be different from the ones described in the book.

There are tens of different manufacturers of AC drives, each offering many different models. The selection of the three AC drives for comparison in this thesis was highly subjective, and the range of candidates was narrow. On the AC drive market, there may very well be models with a whole lot more security and safety related features as in the three products compared in this thesis. Therefore, the results of this study do not represent offerings of the whole AC drive market.

Furthermore, findings during the empirical studies with the AC drives are only applicable with the exact system specifications detailed in Appendix B. Important to this are the option modules, hardware revisions, and firmware and software versions. Due to constant product engineering, exactly the same configurations of the AC drives may not be available from the manufacturers anymore.

Due to existence of newer software versions available regarding some of the tools, it is possible that some of the older versions of the software used in this thesis had bugs, i.e. programming flaws, which might even be so significant that they could have an effect on the results. For example, some tools for remote exploits (such as Metasploit modules) could only work properly with the latest versions. Also, there are newer firmware versions available for the AC drives studied in this thesis. However, older versions are usually more susceptible to exploits than updated versions, so in that sense the AC drives used express a worser case for cybersecurity.

The test setup used with the AC drives did not correspond to normal use case, because the usual upper control systems such as PLCs were not used. Furthermore, fieldbus communication was not set up according to normal standards with cyclic communication between the IED and the PLC. Therefore, all related aspects were not covered.

8.5.3 Further Studies

This thesis focused on one industrial AC drive application: the decanter centrifuge. The results can be applied at least to other centrifuges controlled by AC drives. However, there are many other applications also. Further studies with other AC drive applications could point out similarities in respect to the decanter and/or centrifuge vulnerabilities, but also differences requiring other kinds of protection methods.

One important and widely used AC drive application is used in sewerage systems: the sewage pump. There has been at least one publicly known attack against those pumps (the Maroochy Shire case presented in Section 2.2.3). Advanced AC drives offer features such as process variable (proportional–integrative–derivative, PID) control, which could be utilized to monitor and protect against sewage overflow.

Naturally, in respect to any business, customer demands are an important issue. Unfortunately, no actual customers for AC drive manufacturers were interviewed for this thesis. It would be very beneficial for both parties (customers and suppliers) to study customer opinions, views, and wishes regarding security features of AC drives.

Furthermore, it could be even more important to focus on the customers for decanter centrifuges. After all, they are the end-users connecting decanters to a network of a plant. Nevertheless, many parties are involved in industrial automation including vendors, operators, and contractors, who all should be taken into account for a comprehensive approach.

Standards related to security of industrial control systems were not thoroughly analyzed in this thesis. However, they can be very important in the future, especially if they are to be enforced similarly to NERC CIP (discussed in Section 5.2.4). Therefore, it is recommended to further study the requirements and recommenda-

tions of different standards and similar articles in respect to AC drives and decanter centrifuges.

The vulnerability assessment of AC drives in this thesis was barely a scratch of the surface. Therefore, more extensive vulnerability assessments and evaluations of AC drives, similar to those done to PLCs by security experts recently (e.g. by Beresford [2011]), could bring important issues to daylight. Instead of assessing multiple AC drives for comparison at once, like was done in this thesis, more extensive results could be achieved by focusing on a single AC drive at a time. Better results can also be achieved with commercial tools for vulnerability assessments, which were not used in this thesis.

Then, there is also the issue affecting the whole network industry: IPv6. None of the AC drives studied in this thesis supported IPv6 (128-bit) addressing. Following the evolution of other network devices, it is possible (and even probable) that IPv6 implementations will be seen in AC drives, sooner or later. However, despite IPv6 bringing security features, it also bears many risks such as the potentially increased Internet exposure with direct, public IP addressing, and problems with IPv6 network stacks as seen with other systems (even in the security-focused OS called *OpenBSD* [Hartmeier, 2007]). Therefore, it is recommended to start studying the effects of IPv6 to AC drives as soon as possible. Of course, this also applies to other embedded devices which will be networked.

9 Summary

In essence, this thesis had two main research points: Firstly, to protect the decanter centrifuge from physical destruction despite any possible references supplied to AC drives. "Hazardous" references can reach the drive by whatever means which do not matter in the end. Secondly, to conduct informal vulnerability assessment of AC drives, to find potential "holes" which could be exploited to circumvent protection (safety) functions.

The driver for this thesis was the increased threat against industrial control systems, namely due to evolution of malware peaking to Stuxnet in 2010. For starters in this thesis, the Stuxnet case was analyzed. As a result of that, it was discovered that Stuxnet disabled standard protection functions of AC drives by parameter modifications through fieldbus. Then, it was possible to run the gas centrifuges at such high speeds that they were damaged due to centrifugal forces.

Next, the main industrial AC drive application subject, the decanter centrifuge, was analyzed, focusing on vulnerabilities in its distinct components: the solid-bowl, scroll-discharge centrifuge, the induction motor, and the AC drive. Consequently, it was found out that the decanter must be protected at least from overspeeds.

Stuxnet has shown that parameter modifications over fieldbus can result to critical situations in terms of machine condition. Centrifuges are required to have strong casing to hold fragments after rotor rupture, at least according to European standards. If the parameter writes can not be disabled, the only way to prevent overspeed in Stuxnet-like attack is to have safe speed monitoring device, which prevents entry into critical speeds. The safety system is also mandatory according to standards.

Security and safety issues were discussed. Even though being two different things, security and safety are linked together in industrial automation and control systems, because often they share the same technology.

Functional safety was presented according to standards. The safely-limited speed (SLS) function was selected as suitable solution for protection of the decanter centrifuge.

Even the standards require that safety functions are protected from unauthorized modification. Three selected AC drives from different manufacturers, with functional safety features and Ethernet-based fieldbus connectivity, were compared and their security and safety features evaluated. Features specific to security were few in the AC drives. Although all of them provided the possibility to protect safety configuration by a password, complexity requirements for the password were low.

No major vulnerabilities were found in any of the three AC drives during the brief study in this thesis, apart from the most obvious one which is related to the unfortunate legacy of traditional fieldbuses: total configuration, including modifying most settings and restoring the device to factory defaults, is possible through fieldbus without any form of authentication. Fieldbuses were originally designed for closed networks. This *insecure-by-design* issue still plagues even the modern field devices such as AC drives. Positively, driven by the requirement for compliance with standards, functional safety settings can be protected by simple passwords, however, even that does not protect from restoring factory defaults in all cases.

Nevertheless, by using *defense-in-depth* strategy with multiple layers of different security and safety measures, it is possible to protect the decanter centrifuge from cyber sabotage. Unfortunately, it may not be possible to remotely monitor the safety devices in all cases. Like a double-edged sword, remote monitoring brings good and bad things along with it. Therefore, totally isolated safety instrumented systems are still justifiable, at least in the most critical applications and environments.

For most decanter centrifuge applications using AC drives, the security checklist (Appendix C) provides a good starting point and a basis for which OEMs and other parties can build their own security procedures. In addition to documentation and procedures, proper training of personnel is of utmost importance in dealing with security issues. Many recent, advanced cyber attacks have begun by a simple social engineering method with an email attachment, which, when opened, compromises the whole network.

News about industrial cybersecurity incidents are published, at least seemingly, at increasing rate. It may very well be, that right after this thesis has been published, a "2nd generation Stuxnet" (or 3rd, or 4th, etc.) is discovered, probably revealing even more elaborate techniques for sabotage. Hopefully properly secured safety systems are in place when that happens, and casualties can be avoided.

References

ABB. *Low voltage motors Manual*. D revision, web edition, 2010a. URL http://www05.abb.com/global/scot/scot259.nsf/veritydisplay/e91c4310d39e913ac12577fc003278fb/$file/Standard_LV_Motors_Manual_EN_01_2009%20Rev%20D.pdf. Cited January 25, 2013. 26 pages.

ABB. *Security for Industrial Automation and Control Systems*. B revision, web edition, October 22, 2010b. URL http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/b1f29a78bc9979d7c12577ec00177633/$file/3BSE032547_B_en_Security_for_Industrial_Automation_and_Control_Systems.pdf. Cited January 21, 2013. 16 pages.

ABB. *Low voltage process performance motors catalog*. C revision, web edition, 2011a. URL http://www05.abb.com/global/scot/scot234.nsf/veritydisplay/c4fabac2479e4a1dc125798a0024d79d/$file/catalog%20process%20perf%209akk104556%20en%2005_2011%20revc.pdf. Cited January 25, 2013. 123 pages.

ABB. All-compatible ABB drives: Designed to optimize every kilowatt and maximize output. Web document, April 4, 2011b. URL http://www.abb.de/cawp/seitp202/69e3d67432de968fc125786300486731.aspx. Cited October 22, 2012.

ABB. Drive composer. Web document, 2012a. URL http://www.abb.com/product/seitp322/5a265ca6dcca8b70c12579430024e228.aspx. Cited November 13, 2012.

ABB. *ABB drives and motors for improving energy efficiency*. B revision, web edition, 2012b. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/06089e41600d59b3c1257a130024f543/$file/EN_ABB_drives_and_motors_energy_efficiency_REVB.pdf. Cited January 25, 2013. 15 pages.

ABB. ABB image bank. Web document, 2012c. Cited January 25, 2013.

ABB. *ACS880, single drives 0.55 to 250 kW Catalog*. E revision, web edition, 2012d. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/b985e25a92723a56c12579e90023e0a5/$file/en_acs880_single_drives_reve.pdf. Cited January 25, 2013. 31 pages.

ABB Ltd. ABB Parts OnLine: 3AUA0000131038 ZMU-01 old SW version memory unit kit. Web document, 2010. URL http://194.241.163.244/statim/fiser103.nsf/all%20spares/FISER3AUA0000131038. Cited January 15, 2013.

ABB Ltd. ABB glossary of technical terms. Web document, February 14, 2011. URL http://www.abb.com/glossary. Cited August 24, 2012.

ABB Ltd. Drive PC tools. Web document, 2012. URL http://www.abb.com/product/us/9AAC113388.aspx. Cited January 17, 2013.

ABB Oy. *FEN-11 Absolute Encoder Interface User's Manual*. C revision, web edition, April 20, 2007. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/e9bf78507e5f76bdc12572d00023fbbe/$file/en_fen_11_um_c.pdf. Cited January 25, 2013. 38 pages.

ABB Oy. *FPBA-01 PROFIBUS DP adapter module User's manual*. E revision, web edition, September 07, 2011a. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/280ac0b336e9da83c125790a00485e97/$file/en_fpba01_um_e_screenres.pdf. Cited January 27, 2013. 172 pages.

ABB Oy. *FENA-01/-11 Ethernet adapter module User's manual*. A revision, web edition, September 07, 2011b. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/74152fb1ab82ab43c125790a00496499/$file/en_fena01_11_um_a_screenres.pdf. Cited January 25, 2013. 356 pages.

ABB Oy. *FSO-11 safety functions module User's manual DRAFT*, January 11, 2012a. 154 pages.

ABB Oy. *Drive composer start-up and maintenance PC tool user's manual*. C revision, web edition, September 27, 2012b. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/81dfaeda767cb97cc1257a8600269bfe/$file/DC%20start-up%20and%20maint_PC%20tool%20UM_REV%20C_commenting%20enabled.pdf. Cited January 25, 2013. 116 pages.

ABB Oy. *ACS880 Primary Control Program Firmware Manual*. E revision, web edition, November 5, 2012c. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/1b406dc57f3c26d1c1257aaf003f3dcf/$file/EN_ACS880_FW_Man_E.pdf. Cited January 25, 2013. 370 pages.

ABB Oy. *FSO-11 safety functions module User's manual*. C revision, web edition, October 31, 2012d. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/16a5c217f72ecaa4c1257aa80066ab5a/$file/EN_FSO_11_UM_C.pdf. Cited January 25, 2013. 160 pages.

ABB Oy. *ACS880-01 drives (0.55 to 250 kW, 0.75 to 350 hp) Hardware manual*. E revision, web edition, June 29, 2012e. URL http://www05.abb.com/global/scot/scot201.nsf/veritydisplay/4df11f8cd09f0539c1257a2b005f2ae0/$file/en_ACS880_01_HW_rev_E_scrres.pdf. Cited January 25, 2013. 192 pages.

Abdollahy, R. Calendars. *Encyclopædia Iranica*, web edition, Vol. IV, Fasc. 6–7: 658–677, December 15, 1990. URL http://www.iranicaonline.org/articles/calendars. Cited January 25, 2013.

Abrams, M. and Weiss, J. *Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia*, web edition, July 23, 2008. URL http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf. Cited November 14, 2012. 16 pages.

Al Jazeera. Iran 'briefly halted enrichment'. *Al Jazeera*, web edition, November 23, 2010. URL http://www.aljazeera.com/news/middleeast/2010/11/201011231936673748.html. Cited October 15, 2012.

Albright, D. and Hibbs, M. Iraq's shop-till-you-drop nuclear program. *The Bulletin of the Atomic Scientists*, web edition, 48(3):26–37, April 1992. URL http://books.google.com/books?id=cgsAAAAAMBAJ&pg=PA26. Cited January 25, 2013.

Albright, D. and Walrond, C. *Iran's Gas Centrifuge Program: Taking Stock*. Institute for Science and International Security, Washington, DC, web edition, February 11, 2010. URL http://isis-online.org/uploads/isis-reports/documents/Natanz_Operation_11Feb2010.pdf. Cited July 16, 2012. 26 pages.

Albright, D. and Walrond, C. *Performance of the IR-1 Centrifuge at Natanz*. Institute for Science and International Security, web edition, October 18, 2011. URL http://isis-online.org/uploads/isis-reports/documents/IR1_Centrifuge_Performance_18October2011.pdf. Cited July 16, 2012. 7 pages.

Albright, D., Brannan, P., and Walrond, C. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security, Washington, DC, web edition, December 22, 2010. URL http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf. Cited July 16, 2012. 10 pages.

Albright, D., Brannan, P., and Walrond, C. *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Institute for Science and International Security, Washington, DC, web edition, February 15, 2011. URL http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf. Cited June 27, 2012. 12 pages.

Alfa Laval. *P2 decanter centrifuge range—High-performance decanter centrifuge for process industries*, web edition, 2006. URL http://www.alfalaval.com/solution-finder/products/p2-range/Documents/P2%20decanter%20centrifuge%20range.pdf. Cited September 20, 2012.

Alfa Laval Corporate AB. High performance decanter. Web document, September 13, 2003. URL http://www.alfalaval.com/about-us/press/product-press/Pages/nx-400.aspx. Cited October 8, 2012.

Alfa Laval Corporate AB. *Decanter Range for Process Industries*. Lund, web edition, March 2007. URL http://www.alfalaval.com/about-us/press/product-press/Documents/071030_p2_decanters_en.pdf. Cited September 20, 2012. 3 pages.

Alfa Laval Corporate AB. *Alfa Laval—decanter centrifuge technology*, web edition, 2008. URL http://local.alfalaval.com/en-us/key-technologies/separation/separators/dafrecovery/Documents/Alfa_Laval_decanter_centrifuge_technology.pdf. Cited January 18, 2013. 14 pages.

Alfa Laval Corporate AB. Alfa Laval at ACHEMA 2012—sharing recipes for success. Web document, April 2012. URL http://www.alfalaval.com/campaigns/achema/press/press-releases/Pages/press-releases.aspx. Cited September 20, 2012.

Alfa Laval Corporation. Alfa Laval in the USA. Web document, 2012. URL http://local.alfalaval.com/en-us/about-us/alfa-laval-usa/pages/default.aspx. Cited August 23, 2012.

Alibaba.com Hong Kong Limited. Rotary encoder products. Web document, 2012. URL http://www.alibaba.com/trade/search?SearchText=rotary+encoder. Cited October 11, 2012.

Andress, J. and Winterfield, S. *Cyber Warfare*. Elsevier, Waltham, 2011. 289 pages.

BackTrack Linux. BackTrack Linux—penetration testing distribution. Web document, 2011a. URL http://www.backtrack-linux.org/. Cited November 13, 2012.

BackTrack Linux. BackTrack 5 release. Web document, May 10, 2011b. URL http://www.backtrack-linux.org/backtrack/backtrack-5-release/. Cited January 3, 2013.

BackTrack Linux. BackTrack 5 R3 released! Web document, August 13, 2012a. URL http://www.backtrack-linux.org/backtrack/backtrack-5-r3-released/. Cited November 12, 2012.

BackTrack Linux. About BackTrack. Web document, 2012b. URL http://www.backtrack-linux.org/about/. Cited November 12, 2012.

Baldwin, R. Apple confirms suspension of over-the-phone password resets. *Wired*, web edition, August 8, 2012. URL http://www.wired.com/gadgetlab/2012/08/apple-confirms-it-has-suspended-over-the-phone-appleid-password-resets/. Cited December 23, 2012.

Beaty, H. W. and Kirtley, J. L. Jr. *Electric Motor Handbook*. McGraw-Hill, New York, 1998. 404 pages.

Beresford, D. Exploiting Siemens Simatic S7 PLCs. In *Black Hat USA*, web edition, Las Vegas, July 8, 2011. URL http://scadahacker.com/files/reference/BH_US11_Beresford_S7_PLCs_WP.pdf. Cited January 11, 2013. 26 pages.

Blankenship, L. The conscience of a hacker. *Phrack*, web magazine, 1(7):3, September 25, 1986. URL http://www.phrack.org/issues.html?issue=7&id=3. Cited August 20, 2012.

Boyes, W. Cybersecurity in your safety DNA. *Control Global*, web edition, May 7, 2012. URL http://www.controlglobal.com/articles/2012/boyes-cybersecurity-safety-dna.html. Cited January 2, 2013.

Broad, W. J. Slender and elegant, it fuels the bomb. *The New York Times*, web edition, March 23, 2004. URL http://www.nytimes.com/2004/03/23/science/slender-and-elegant-it-fuels-the-bomb.html. Cited July 20, 2012.

Bukharin, O. Understanding Russia's uranium enrichment complex. *Science and Global Security*, web edition, 12:192–218, 2004. URL http://dx.doi.org/10.1080/08929880490521546. Cited September 7, 2012.

Byres, E. and Cusimano, J. Safety and security: Two sides of the same coin. *Control Global*, web edition, March 25, 2010. URL http://www.controlglobal.com/articles/2010/SafetySecurity1004.html. Cited October 1, 2012.

Canonical Ltd. The Ubuntu story. Web document, 2013. URL http://www.ubuntu.com/project/about-ubuntu. Cited January 3, 2013.

Cisco Systems, Inc. Network topology icons. Web document, 2012. URL http://www.cisco.com/web/about/ac50/ac47/2.html. Cited October 19, 2012.

Cisco Systems, Inc. and Rockwell Automation, Inc. *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*, web edition, September 9, 2011. URL http://www.cisco.com/en/US/docs/solutions/Verticals/CPwE/CPwE_DIG.pdf. Cited January 25, 2013. 564 pages.

Comité Européen de Normalisation. European standard EN ISO 13849-1 Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design. Bruxelles, June 2008. 87 pages.

Comité Européen de Normalisation. European standard EN 12547:1999+A1 Centrifuges—Common safety requirements. Bruxelles, March 2009. 52 pages.

Comité Européen de Normalisation. European standard EN ISO 12100:2010 Safety of machinery—General principles for design—Risk assessment and risk reduction. Bruxelles, November 2010. 78 pages.

Coviello, A. Open letter to RSA customers. Web document, 2012. URL http://www.rsa.com/node.aspx?id=3872. Cited September 27, 2012.

DFA Media Ltd. ABB hopes tiny drives will win bigger slice of global market. *Drives & Controls*, web edition, April 2002. URL http://www.drives.co.uk/fullstory.asp?id=1612. Cited November 12, 2012.

DFA Media Ltd. Stuxnet targets Vacon inverters. *Drives & Controls*, web edition, November 2010. URL http://www.drives.co.uk/fullstory.asp?id=3030. Cited October 15, 2012.

Digital Bond, Inc. Rockwell Automation ControlLogix. Web document, 2012a. URL http://www.digitalbond.com/tools/basecamp/rockwell-automation-controllogix/. Cited November 6, 2012.

Digital Bond, Inc. Basecamp. Web document, 2012b. URL http://www.digitalbond.com/tools/basecamp/. Cited September 27, 2012.

Drummond, D. A new approach to China. *Google Official Blog*, web document, January 13, 2010. URL http://googleblog.blogspot.fi/2010/01/new-approach-to-china.html. Cited September 6, 2012.

European Network and Information Security Agency. *Protecting Industrial Control Systems—Recommendations for Europe and Member States*, web edition, December 2011. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states. Cited January 25, 2013. 71 pages.

F-Secure Corporation. About F-Secure. Web document, 2011. URL http://www.f-secure.com/en/web/corporation_global/company/about-f-secure. Cited August 29, 2012.

F-Secure Corporation. *Threat Report H1 2012*, web edition, 2012a. URL http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2012.pdf. Cited October 15, 2012. 39 pages.

F-Secure Corporation. Terminology. Web document, 2012b. URL http://www.f-secure.com/en/web/labs_global/terminology. Cited August 21, 2012.

Falliere, N., O Murchu, L., and Chien, E. *W32.Stuxnet Dossier*. Symantec Corporation, version 1.4, web edition, February 2011. URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Cited June 27, 2012. 68 pages.

Fisher, D. Final report on DigiNotar hack shows total compromise of CA servers. *The Kaspersky Lab Security News Service*, web document, October 31, 2012a. URL http://threatpost.com/en_us/blogs/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112. Cited December 27, 2012.

Fisher, D. What's the meaning of this: Adobe certificate attack. *The Kaspersky Lab Security News Service*, web document, September 28, 2012b. URL http://threatpost.com/en_us/blogs/whats-meaning-adobe-certificate-attack-092812. Cited December 27, 2012.

Follath, E. Interview with former nuclear watchdog: The Iranians 'tricked and misled us'. *DER SPIEGEL*, web edition, June 10, 2011. URL http://www.spiegel.de/international/world/spiegel-interview-with-former-nuclear-watchdog-the-iranians-tricked-and-misled-us-a-790042.html. Cited October 25, 2012.

Frankel, S., Graveman, R., Pearce, J., and Rooks, M. *Guidelines for the Secure Deployment of IPv6*. National Institute of Standards and Technology Special Publication 800-119, Gaithersburg, web edition, December 2010. URL http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf. Cited January 3, 2013. 188 pages.

Free Software Foundation, Inc. GNU general public license. Web document, June 29, 2007. URL http://www.gnu.org/licenses/gpl.html. Cited November 13, 2012.

Gervais, A. Security analysis of industrial control systems. Master's thesis, KTH Stockholm and Aalto University, Espoo, June 29 2012. URL http://nordsecmob.aalto.fi/en/publications/theses_2012/gervais-arthur_thesis.pdf. Cited January 25, 2013. 90 pages.

Glaser, A. Characteristics of the gas centrifuge for uranium enrichment and their relevance for nuclear weapon proliferation (corrected). *Science and Global Security*, web edition, 16:1–25, 2008. URL http://dx.doi.org/10.1080/08929880802335998. Cited September 11, 2012.

GlobalSecurity.org. Natanz (Kashan). Web document, July 24, 2011. URL http://www.globalsecurity.org/wmd/world/iran/natanz.htm. Cited January 14, 2013.

Gollmann, D. *Computer Security*. John Wiley & Sons, West Sussex, third edition, 2011. 436 pages.

Goodin, D. Phishing email used in serious RSA attack surfaces. *The Register*, web magazine, August 26, 2011. URL http://www.theregister.co.uk/2011/08/26/rsa_attack_email_found/. Cited December 27, 2012.

Gottlieb, I. M. *Practical Electric Motor Handbook*. Newnes, Oxford, 1997. 167 pages.

Gruhn, P. and Cheddie, H. L. *Safety Instrumented Systems: Design, Analysis, and Justification*. ISA—The Instrumentation, Systems, and Automation Society, North Carolina, 2nd edition, 2006. 314 pages.

Hafezi, P. Iran admits cyber attack on nuclear plants. *Reuters*, web edition, November 29, 2010. URL http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129. Cited September 11, 2012.

Hagen, S. *IPv6 Essentials*. O'Reilly Media, Sebastopol, second edition, May 2006. 438 pages.

Haglili, O. Elite intelligence unit protects the environment. Web document, 2012. URL http://www.idf.il/1283-17243-en/Dover.aspx. Cited November 19, 2012.

Harnefors, L. Control of variable-speed drives. Västerås, September 11, 2003. 234 pages.

Harris, R. *Modern Physics*. Pearson Addison-Wesley, San Francisco, second edition, 2008. 558 pages.

Hartmeier, D. Only two remote holes in the default install, in more than 10 years! *OpenBSD Journal*, web document, March 14, 2007. URL http://undeadly.org/cgi?action=article&sid=20070314040700. Cited September 12, 2012.

Hawrylak, P. J., Haney, M., Papa, M., and Hale, J. Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In *5th International Symposium on Resilient Control Systems (ISRCS)*, web edition, pages 161–164, Salt Lake City, August 14–16, 2012. URL http://dx.doi.org/10.1109/ISRCS.2012.6309311. Cited January 25, 2013.

Heikkilä, S. *U.S. Patent Number 6,094,364: Direct torque control inverter arrangement*, web edition, 2000. URL http://www.google.com/patents/US6094364. Cited January 25, 2013.

Honan, M. How Apple and Amazon security flaws led to my epic hacking. *Wired*, web edition, August 6, 2012. URL http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking. Cited August 16, 2012.

Huhtinen, P. Information security of industrial control systems. Master's thesis, Aalto University, Espoo, October 10, 2011. 71 pages.

ICS-CERT. *ICS-CERT Fact Sheet*, web edition, 2010. URL http://www.us-cert.gov/control_systems/pdf/ICS_CERT%20Factsheet.pdf. Cited September 27, 2012. 2 pages.

ICS-CERT. *ICS-ALERT-12-020-03B—Schneider Electric Modicon Quantum multiple vulnerabilities*, web edition, April 9, 2012a. URL http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-020-03B.pdf. Cited January 17, 2013. 4 pages.

ICS-CERT. *ICS-ALERT-12-046-01—Increasing threat to industrial control systems*, web edition, February 15, 2012b. URL http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01.pdf. Cited September 27, 2012. 4 pages.

ICS-CERT. ICS-CERT advisories and reports archive. Web document, August 2012c. URL http://www.us-cert.gov/control_systems/ics-cert/archive.html. Cited January 25, 2013.

Institute for Science and International Security. Aluminum tubing is an indicator of an Iraqi gas centrifuge program: But is the tubing specifically for centrifuges? Web document, October 9, 2002. URL http://isis-online.org/isis-reports/detail/aluminum-tubing-is-

an-indicator-of-an-iraqi-gas-centrifuge-program-but-is-t/9. Cited July 17, 2012.

Institute for Science and International Security. What is a gas centrifuge? Web document, 2003. URL http://www.exportcontrols.org/centrifuges.html. Cited September 6, 2012.

Institute for Science and International Security. Biography of David Albright. Web document, 2010. URL http://isis-online.org/about/staff/albright/. Cited September 11, 2012.

Institute for Science and International Security. About ISIS. Web document, 2011. URL http://isis-online.org/about/. Cited September 11, 2012.

Institute of Electrical and Electronics Engineers, Inc. IEEE 802.3-2008—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. New York, web edition, June 22, 2010. URL http://standards.ieee.org/about/get/802/802.3.html. Cited January 25, 2013. 597 pages.

Institute of Electrical and Electronics Engineers, Inc. OUI public listing. Web document, 2013. URL http://standards.ieee.org/develop/regauth/oui/public.html. Cited January 15, 2013.

International Atomic Energy Agency. *Production of Yellow Cake and Uranium Fluorides*. Panel Proceedings Series. Wien, web edition, 1980. URL http://www-pub.iaea.org/books/IAEABooks/3385/Production-of-Yellow-Cake-and-Uranium-Fluorides-Paris-5-8-June-1979. Cited January 25, 2013. 355 pages.

International Atomic Energy Agency. *Annex 3—List of items to be reported to IAEA*. Vienna, web edition, 2001. URL http://www.iaea.org/OurWork/SV/Invo/annex3/annex3_e.pdf. Cited August 15, 2012. 83 pages.

International Atomic Energy Agency. Head of IAEA safeguards welcomes Iran workplan. Web document, August 30, 2007. URL http://www.iaea.org/newscenter/news/2007/workplan_heinonen.html. Cited October 25, 2012.

International Electrotechnical Commission. International standard IEC 61800-2 Adjustable speed electrical power drive systems—Part 2: General requirements—Rating specifications for low voltage adjustable frequency a.c. power drive systems. Genève, 1998. 175 pages.

International Electrotechnical Commission. International standard IEC 61800-4 Adjustable speed electrical power drive systems—Part 4: General requirements—Rating specifications for a.c. power drive systems above 1 000 V a.c. and not exceeding 35 kV. Genève, 2002. 219 pages.

International Electrotechnical Commission. Technical report IEC/TR 61508-0 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 0: Functional safety and IEC 61508. Genève, 2005. 33 pages.

International Electrotechnical Commission. International standard IEC 61800-5-2 Adjustable speed electrical power drive systems—Part 5-2: Safety requirements—Functional. Genève, 2007. 65 pages.

International Telecommunication Union. ITU-T recommendation T.125 Multipoint communication service protocol specification. Web edition, February 6, 1998. URL `http://www.itu.int/rec/T-REC-T.125/`. Cited January 25, 2013. 133 pages.

International Telecommunication Union. ITU-T recommendation X.1205 Overview of cybersecurity. Genève, web edition, April 2008. URL `http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1205`. Cited January 25, 2013. 55 pages.

Kaspersky, E. The man who found Stuxnet—Sergey Ulasen in the spotlight. Web document, November 2, 2011. URL `http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/`. Cited July 5, 2012.

Kawalek, C. New commercial license for Oracle VM VirtualBox. *Oracle's Virtualization Blog*, web document, March 8, 2012. URL `https://blogs.oracle.com/virtualization/entry/new_commercial_license_for_oracle`. Cited November 20, 2012.

Keizer, G. Iran admits Stuxnet worm infected PCs at nuclear reactor. *Computerworld*, web edition, September 27 2010. URL `http://www.computerworld.com/s/article/9188147/Iran_admits_Stuxnet_worm_infected_PCs_at_nuclear_reactor`. Cited October 15, 2012.

Kemp, R. S. Gas centrifuge theory and development: A review of U.S. programs. *Science and Global Security*, web edition, 17:1–19, 2009. URL `http://dx.doi.org/10.1080/08929880802335816`. Cited January 25, 2013.

Åkerberg, J. and Björkman, M. Exploring security in PROFINET IO. In *33rd Annual IEEE International Computer Software and Applications Conference*, web edition, pages 406–412, Seattle, July 20–24, 2009. URL `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5254232`. Cited January 25, 2013.

Khan, A. Q. *Biodata of Dr. A. Q. Khan*, web edition, 2005. URL `http://www.draqkhan.com.pk/dkbdata.pdf`. Cited September 11, 2012.

Knapp, E. D. *Industrial Network Security*. Elsevier, Waltham, 2011. 341 pages.

Kyyrä, J. Hakkuriteholähteet. Handout of course S-81.3100, Teknillinen korkeakoulu, 2009. 213 pages.

Lamarsh, J. R. and Baratta, A. J. *Introduction to Nuclear Engineering*. Prentice-Hall, New Jersey, third edition, 2001. 783 pages.

Langner, R. *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*. Momentum Press, New York, September 2011a. 222 pages.

Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, web edition, 9(3):49–51, May-June 2011b. URL `http://dx.doi.org/10.1109/MSP.2011.67`. Cited January 25, 2013.

Langner, R. Why attack when we can't defend? *The New York Times*, web edition, June 4, 2012. URL `http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/why-attack-when-we-cant-defend`. Cited January 5, 2013.

Langner Communications GmbH. ICS-CERT on Beresford vulns: Flawed analysis, misleading advice. Web document, August 20, 2011. URL `http://www.langner.com/en/2011/08/20/ics-cert-on-beresford-vulns-flawed-analysis-misleading-advice/`. Cited December 30, 2012.

Luomi, J. Control of electric drives addenda. Helsinki University of Technology, March 5, 2009. 49 pages.

Luomi, J. Sähkökäyttöjen suunnittelu. Handout of course S-81.3310, Espoo, September 2010. 190 pages.

Luomi, J. and Niemenmaa, A. Sähkömekaniikka ja sähkökäytöt. Handout of course S-17.2020, Espoo, January 2011. 226 pages.

Lyon, G. F. *The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC, web edition, 2011. URL `http://nmap.org/book/toc`. Cited November 9, 2012.

Macaulay, T. and Singer, B. *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Taylor & Francis Group, Boca Raton, December 2012. 185 pages.

Marrs, T. A worm in the centrifuge. *The Economist*, web edition, September 30, 2010. URL `http://www.economist.com/node/17147818`. Cited June 29, 2012.

Marshall, P. S. and Rinaldi, J. S. *Industrial Ethernet—How to Plan, Install, and Maintain TCP/IP Ethernet Networks: The Basic Reference Guide for Automation and Process Control Engineers*. ISA—The Instrumentation, Systems, and Automation Society, North Carolina, 2nd edition, 2004. 117 pages.

McMillan, R. Siemens warns users: Don't change passwords after worm attack. *InfoWorld*, web magazine, July 20, 2010. URL `http://www.infoworld.com/d/security-central/siemens-warns-users-dont-change-passwords-after-worm-attack-915`. Cited September 11, 2012.

Merkl, R. and Steiger, W. Properties of decanter centrifuges in the mining industry. *Minerals & Metallurgical Processing*, web edition, 29(1):6–12, February 2012. Cited January 25, 2013.

Merriam-Webster, Inc. Security. Web document, 2012a. URL `http://www.merriam-webster.com/dictionary/security`. Cited November 19, 2012.

Merriam-Webster, Inc. Safety. Web document, 2012b. URL `http://www.merriam-webster.com/dictionary/safety`. Cited November 19, 2012.

Microsoft. Enhanced mitigation experience toolkit v3.0. Web document, 2013a. URL `http://www.microsoft.com/en-us/download/details.aspx?id=29851`. Cited January 23, 2013.

Microsoft. Run only allowed Windows applications. Web document, 2013b. URL `http://msdn.microsoft.com/en-us/library/ms811966.aspx`. Cited January 23, 2013.

Modarres, M., Vahedi, A., and Ghazanchaei, M. Effect of air gap variation on characteristics of an axial flux hysteresis motor. In *Power Electronic & Drive Systems & Technologies Conference (PEDSTC)*, web edition, pages 323–328, Tehran, February 17–18, 2010. URL `http://dx.doi.org/10.1109/PEDSTC.2010.5471798`. Cited January 25, 2013.

National Institute of Standards and Technology. National vulnerability database (NVD) Search vulnerabilities. Web document, 2012. URL `http://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=last3months&cves=on`. Cited November 6, 2012.

Niasar, A. H. and Moghbelli, H. Sensitivity analysis to the design parameters of a hysteresis motor. In *Power Electronics and Drive Systems Technology (PEDSTC)*, web edition, pages 74–78, Tehran, February 15–16, 2012. URL `http://dx.doi.org/10.1109/PEDSTC.2012.6183301`. Cited January 25, 2013.

Niiranen, J. *Sähkömoottorikäytön digitaalinen ohjaus*. Yliopistokustannus/Otatieto, Helsinki, second edition, 2000. 381 pages.

North American Electric Reliability Corporation. Reliability standards. Web document, 2012. URL `http://www.nerc.com/page.php?cid=2|20`. Cited November 5, 2012.

Obama, B. H. Remarks by the President on securing our nation's cyber infrastructure. Web document, May 29, 2009. URL `http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure`. Cited September 28, 2012.

Offensive Security. The Exploit Database. Web document, 2012. URL `http://www.exploit-db.com/`. Cited November 6, 2012.

Offensive Security Ltd. BackTrack Linux. Web document, 2012a. URL http://www.offensive-security.com/community-projects/backtrack-linux/. Cited November 13, 2012.

Offensive Security Ltd. Metasploit Unleashed. Web document, 2012b. URL http://www.offensive-security.com/metasploit-unleashed/Main_Page. Cited November 9, 2012.

Offensive Security Ltd. The Offensive Security team. Web document, 2012c. URL http://www.offensive-security.com/about-us/. Cited November 12, 2012.

Office of the Law Revision Counsel. *The Code of Laws of the United States of America*, web edition, April 2012. URL http://uscode.house.gov/pdf/2011/. Cited August 28, 2012.

Olivarez-Giles, N. Amazon quietly closes security hole after journalist's devastating hack. *Wired*, web edition, August 7, 2012. URL http://www.wired.com/gadgetlab/2012/08/amazon-changes-policy-wont-add-new-credit-cards-to-accounts-over-the-phone/. Cited December 23, 2012.

Open DeviceNet Vendor Association, Inc. *EtherNet/IP Quick Start for Vendors Handbook*. Ann Arbor, web edition, 2008. URL http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00213R0_EtherNetIP_Developers_Guide.pdf. Cited January 25, 2013. 41 pages.

Open DeviceNet Vendor Association, Inc. Member roster. Web document, 2012. URL http://www.odva.org/Home/ABOUTODVA/TheODVACommunity/MemberRoster/tabid/115/lng/en-US/language/en-US/Default.aspx. Cited November 6, 2012.

Open Source Vulnerability Database. OSVDB: The Open Source Vulnerability Database. Web document, 2012. URL http://osvdb.org/. Cited November 6, 2012.

Oracle Corporation. Oracle VM VirtualBox. Web document, 2012a. URL https://www.virtualbox.org/. Cited November 19, 2012.

Oracle Corporation. Licensing: Frequently asked questions. Web document, 2012b. URL https://www.virtualbox.org/wiki/Licensing_FAQ. Cited November 20, 2012.

Oracle Corporation. Download VirtualBox. Web document, 2012c. URL https://www.virtualbox.org/wiki/Downloads. Cited November 20, 2012.

Parviainen, A. Design of axial-flux permanent-magnet low-speed machines and performance comparison between radial-flux and axial-flux machines. Doctoral thesis, Lappeenranta University of Technology, Lappeenranta, web edition, 2005. URL http://www.doria.fi/bitstream/handle/10024/31185/TMP.objres.74.pdf. Cited January 25, 2013. 153 pages.

Poidl, J. and Steiger, W. Variable speed drives and centrifuges for zone 1 hazardous areas. In *Petroleum and Chemical Industry Conference Europe—Electrical and Instrumentation Applications*, web edition, pages 1–8, Weimar, June 10–12, 2008. URL http://dx.doi.org/10.1109/PCICEUROPE.2008.4563524. Cited January 25, 2013.

PROFIBUS Nutzerorganisation e.V. *PROFINET System Description—Technology and Application*. Karlsruhe, web edition, June 2011. URL http://www.profibus.com/nc/downloads/downloads/profinet-technology-and-application-system-description/display/. Cited October 22, 2012. 22 pages.

PROFIBUS Nutzerorganisation e.V. *PROFINET—networking the world with the leading Industrial Ethernet standard*. Karlsruhe, web edition, November 13, 2012. URL http://www.profibus.com/nc/downloads/downloads/profinet/display/. Cited January 25, 2013. 6 pages.

Rapid7. History of the Metasploit Project. Web document, 2012a. URL http://www.metasploit.com/about/history/. Cited November 9, 2012.

Rapid7. Metasploit compare editions. Web document, 2012b. URL http://www.rapid7.com/products/metasploit/compare-editions.jsp. Cited November 21, 2012.

Rapid7. Metasploit 4.5.1 (update 2013011601). Web document, January 17, 2013. URL https://community.rapid7.com/docs/DOC-2144. Cited January 24, 2013.

Raymond, E. S. The jargon file. Version 4.4.8, web document, October 1, 2004a. URL http://catb.org/jargon/. Cited August 16, 2012.

Raymond, E. S. The jargon file revision history. Web document, October 1, 2004b. URL http://catb.org/jargon/html/revision-history.html. Cited August 29, 2012.

Records, A. and Sutherland, K. *Decanter Centrifuge Handbook*. Elsevier Advanced Technology, Oxford, first edition, 2001. 421 pages.

Reid, A. Stuxnet—the first cyberweapon. Web document, June 19, 2012. URL http://www.stpaulsschool.org.uk/resource.aspx?id=247374. Cited September 10, 2012.

Reynders, D. and Wright, E. *Practical TCP/IP and Ethernet Networking*. Newnes, Oxford, 2003. 306 pages.

Riverbed Technology. WinPcap. Web document, 2012. URL http://www.winpcap.org/. Cited January 3, 2013.

Roberts, P. Bloody valentine for critical infrastructure: EtherNet/IP exploit could crash devices. *Threatpost—Kaspersky Lab Security News Service*, web document, February 14, 2012. URL http://threatpost.com/en_us/blogs/

bloody-valentine-critical-infrastructure-ethernet-exploit-could-crash-devices-021412. Cited November 6, 2012.

Rockwell Automation, Inc. Rockwell Automation announces availability of integrated motion on EtherNet/IP portfolio. Web document, November 11, 2009. URL http://phx.corporate-ir.net/phoenix.zhtml?c=196186&p=irol-newsArticle&ID=1354921. Cited October 22, 2012.

Rockwell Automation, Inc. *PowerFlex 750-Series AC Drives*. USA, web edition, October 2011. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/pp/750-pp001_-en-p.pdf. Cited September 6, 2012. 8 pages.

Rockwell Automation, Inc. *Safe Speed Monitor Option Module for PowerFlex 750-Series AC Drives Safety Reference Manual*. Allen-Bradley, U.S.A., web edition, February 2012a. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/rm/750-rm001_-en-p.pdf. Cited January 25, 2013. 182 pages.

Rockwell Automation, Inc. *PowerFlex 750-Series AC Drives Installation Instructions*. U.S.A., web edition, March 2012b. URL https://mail.nelson-electric.com/webshare/Glenn/750-in001_-en-p.pdf. Cited January 25, 2013. 223 pages.

Rockwell Automation, Inc. Allen-Bradley web updates. Web document, 2012c. URL http://www.ab.com/support/abdrives/webupdate/index.html. Cited October 16, 2012.

Rockwell Automation, Inc. *DriveExplorer Discontinuation Notice / Version 6.04.99 Freeware*, web edition, 2012d. URL http://www.ab.com/support/abdrives/webupdate/software/DriveExplorer_Discontinuation_Notice.pdf. Cited November 13, 2012. 1 page.

Rockwell Automation, Inc. Connected Components Workbench software. Web document, 2012e. URL http://ab.rockwellautomation.com/Programmable-Controllers/Connected-Components-Workbench-Software. Cited November 14, 2012.

Rockwell Automation, Inc. *DriveExplorer Version 6.04 Release Notes*. U.S.A., web edition, April 2012f. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/rn/9306-rn008_-en-p.pdf. Cited November 14, 2012. 4 pages.

Rockwell Automation, Inc. *PowerFlex 755 Drive Embedded EtherNet/IP Adapter User Manual*. U.S.A., web edition, February 2012g. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/um/750com-um001_-en-p.pdf. Cited January 25, 2013. 248 pages.

Rockwell Automation, Inc. *PowerFlex 1203-USB Converter User Manual*. USA, web edition, September 2012h. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/um/drives-um001_-en-p.pdf. Cited January 25, 2013. 106 pages.

Rockwell Automation, Inc. *PowerFlex 755 Drives (revision 7.001) Release Notes*. USA, web edition, September 2012i. URL http://www.ab.com/support/abdrives/webupdate/firmware/notes/PF755_App_v7_001_026_ControlFLASH.pdf. Cited December 22, 2012. 24 pages.

Rockwell Automation, Inc. *PowerFlex 750-Series AC Drives Reference Manual*. U.S.A., web edition, September 2012j. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/rm/750-rm002_-en-p.pdf. Cited January 25, 2013. 342 pages.

Rockwell Automation, Inc. *PowerFlex 750-Series Safe Torque Off User Manual*. U.S.A., web edition, February 2012k. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/um/750-um002_-en-p.pdf. Cited January 25, 2013. 36 pages.

Rockwell Automation, Inc. *PowerFlex 750-Series AC Drives Programming Manual*. U.S.A., web edition, September 2012l. URL http://literature.rockwellautomation.com/idc/groups/literature/documents/pm/750-pm001_-en-p.pdf. Cited January 25, 2013. 510 pages.

Rogers, M. and Ruppersberger, C. D. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. U.S. House of Representatives, web edition, October 8, 2012. URL http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf. Cited November 13, 2012. 52 pages.

Rose, M. T. and Cass, D. E. RFC 1006 ISO transport service on top of the TCP. Version: 3, web document, May 1987. URL http://tools.ietf.org/html/rfc1006. Cited January 25, 2013. 18 pages.

Sanders, C. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. No Starch Press, San Francisco, 2007. 164 pages.

Sanger, D. E. Obama order sped up wave of cyberattacks against Iran. *The New York Times*, web edition, June 1, 2012. URL http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Cited June 28, 2012.

Schmidt, M. S., Bradsher, K., and Hauser, C. U.S. panel cites risks in Chinese equipment. *The New York Times*, web edition, October 9, 2012. URL http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html. Cited November 13, 2012.

Siemens AG. *Drive line extended by single-axis servo converter*. Nürnberg, web edition, November 24, 2008. URL http://www.siemens.com/press/pool/de/pressemitteilungen/drive_technologies/idt2008111729e.pdf. Cited October 22, 2012. 4 pages.

Siemens AG. *Basic Operator Panel 20 (BOP20) Operating Instructions*. Nürnberg, web edition, May 2010. URL http://support.automation.siemens.com/WW/view/en/35126959. Cited January 25, 2013. 26 pages.

Siemens AG. *SINAMICS S110 Manual*. Erlangen, web edition, January 2011a. URL http://support.automation.siemens.com/WW/view/en/49086218. Cited January 25, 2013. 315 pages.

Siemens AG. *SINAMICS S110 Function Manual*. Nürnberg, web edition, January 2011b. URL http://www.industry.usa.siemens.com/datapool/us/DT/Drives/docs/DRV-SINAMICS_S110-Function_Manual.pdf. Cited January 25, 2013. 730 pages.

Siemens AG. *SINAMICS and Motors for Single-Axis Drives*. Erlangen, web edition, 2011c. URL http://www.automation.siemens.com/mcms/infocenter/dokumentencenter/mc/Documentsu20Catalogs/Catalog-D31-2012-en.pdf. Cited January 25, 2013. 450 pages.

Siemens AG. Expanded range of controllers with increased performance and more compact design. Web document, February 23, 2011d. URL http://www.siemens.com/ia-picture/2521. Cited October 23, 2012.

Siemens AG. 6SL3040-0JA01-0AA0 S110 control unit CU305 PN. Web document, 2012a. URL http://support.automation.siemens.com/WW/view/en/44211566. Cited October 22, 2012.

Siemens AG. *SINAMICS S110 List Manual*. Erlangen, firmware version 4.4, web edition, June 2012b. URL http://cache.automation.siemens.com/dnl/Tk/TkzMDE3NQAA_62999674_HB/LH7_0612_eng.pdf. 1286 pages.

Siemens AG. Drive ES—Starter V4.3.1.2. Help file, 2012c.

Siemens AG. SIMATIC STEP 7: the comprehensive engineering system. Web document, 2012d. URL http://www.automation.siemens.com/mcms/simatic-controller-software/en/step7/pages/default.aspx. Cited December 21, 2012.

Siemens AG. *SSA-027884: Insecure SQL Server Authentication in SIMATIC WinCC*. Siemens ProductCERT, web edition, July 23, 2012e. URL https://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-027884.pdf. Cited September 11, 2012. 2 pages.

Siemens AG. SINAMICS MICROMASTER STARTER. Web document, 2012f. URL http://support.automation.siemens.com/WW/view/en/10804985/133100. Cited November 13, 2012.

Siemens AG. New primary setup tool (PST) version 4.1 and new version V3.2 or 4.0 for address setting of SIMATIC NET Industrial Ethernet products available for download. Web document, May 28, 2012g. URL http://support.automation.siemens.com/US/view/en/19440762. Cited December 21, 2012.

Siemens AG. *SINAMICS S110*. Erlangen, web edition, March 2012h. URL https://c4b.gss.siemens.com/resources/articles/e20001-a40-p670-v2-7600.pdf. Cited January 25, 2013. 8 pages.

Siemens AG. SINAMICS MMC 6SL3054-4EE00-0AA0. Web document, 2013. URL http://support.automation.siemens.com/WW/view/en/48333878. Cited January 15, 2013.

sKyWIper Analysis Team. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Budapest University of Technology and Economics, web edition, May 31, 2012. URL http://www.crysys.hu/skywiper/skywiper.pdf. Cited July 2, 2012. 64 pages.

Smith, T. Hacker jailed for revenge sewage attacks. *The Register*, web magazine, October 31, 2001. URL http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/. Cited November 14, 2012.

Software in the Public Interest, Inc. Debian security information. Web document, November 5, 2012a. URL http://www.debian.org/security/. Cited November 7, 2012.

Software in the Public Interest, Inc. Who's using Debian? Web document, November 1, 2012b. URL http://www.debian.org/users/. Cited January 3, 2013.

Sogg, D. Decanting. *Wine Spectator Online*, web document, November 15, 2003. URL http://www.winespectator.com/wssaccess/show/id/40856. Cited November 2, 2012.

Stouffer, K., Falco, J., and Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology Special Publication 800-82, Gaithersburg, web edition, June 2011. URL http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf. Cited January 25, 2013. 155 pages.

Strategic Cyber LLC. Download Armitage. Web document, 2012. URL http://www.fastandeasyhacking.com/download. Cited January 4, 2013.

Strategic Cyber LLC. Armitage manual. Web document, 2013a. URL http://www.fastandeasyhacking.com/manual. Cited January 4, 2013.

Strategic Cyber LLC. Advanced penetration testing software—Cobalt Strike. Web document, 2013b. URL http://www.advancedpentest.com/. Cited January 4, 2013.

Sundell, M., Kuivalainen, J., Mäkelä, J., Gervais, A., Orava, J., and Hyppönen, M. H. *White Paper on Industrial Automation Security in Fieldbus and Field Device Level*. Vacon Plc, web edition, December 9, 2011. URL http://www.vacon.com/Vacon-White-Paper-On-Industrial-Automation-Security-In-Fieldbus-And-Field-Device-Level.pdf. Cited June 27, 2012. 43 pages.

Symantec Corporation. *W32.Duqu The precursor to the next Stuxnet*. Version 1.4, web edition, November 23, 2011. URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf. Cited July 2, 2012. 71 pages.

Symantec Corporation. SecurityFocus. Web document, 2012a. URL http://www.securityfocus.com/. Cited November 6, 2012.

Symantec Corporation. Corporate profile. Web document, 2012b. URL http://www.symantec.com/about/profile/. Cited November 16, 2012.

Symantec Corporation. W32.Flamer. Web document, June 5, 2012c. URL http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99. Cited October 15, 2012.

The Hacker's Choice. The Hacker's Choice. Web document, 2008. URL http://www.thc.org/. Cited January 3, 2013.

The Hacker's Choice. THC-Hydra. Web document, December 24, 2012a. URL http://www.thc.org/thc-hydra/. Cited January 3, 2013.

The Hacker's Choice. Changelog for hydra. Web document, 2012b. URL http://www.thc.org/thc-hydra/CHANGES. Cited January 3, 2013.

Tiger Security S.r.l. Tiger Security S.r.l. Web document, 2012. URL http://www.tigersecurity.it/. Cited November 12, 2012.

Tiitinen, P. and Surandra, M. The next generation motor control method, DTC direct torque control. In *International Conference on Power Electronics, Drives and Energy Systems for Industrial Growth*, web edition, pages 37–43, New Delhi, January 8–11, 1996. URL http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=537279. Cited January 25, 2013.

TrustedSec, LLC. About us. Web document, 2012. URL https://www.trustedsec.com/about-us/. Cited December 23, 2012.

Underwriters Laboratories Inc. UL 508C Standard for Safety for Power Conversion Equipment. Third edition, 2010. 172 pages.

Union of Concerned Scientists. *Preventing Nuclear Terrorism: Fissile Materials Basics*, web edition, 2004. URL http://www.ucsusa.org/assets/documents/nwgs/nuclear_terrorism-fissile_materials.pdf. Cited August 15, 2012. 2 pages.

Urenco Limited. Centrifuges. Web document, 2012. URL http://www.urenco.com/content/23/centrifuges.aspx. Cited September 6, 2012.

U.S. Department of Energy. A reference book for annex 3 of handbook for notifications of exports to Iraq. Web document, April 1998. URL http://www.iraqwatch.org/government/US/DOE/DOE-Annex3.htm. Cited August 15, 2012.

U.S. Department of Energy. *A Handbook for the International Atomic Energy Agency's Model Additional Protocol Annex II*, web edition, February 2004. URL http://www.jnrc.gov.jo/Publications/USA%20Handbook_Model%20Additional%20Protocol%20Annex%20II.pdf. Cited September 26, 2012. 273 pages.

U.S. Department of Homeland Security. Homeland security presidential directive 7: Critical infrastructure identification, prioritization, and protection. Web document, December 17, 2003. URL http://www.dhs.gov/homeland-security-presidential-directive-7. Cited November 22, 2012.

U.S. Department of Homeland Security. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*. Control Systems Security Program (CSSP), National Cyber Security Division (NCSD), web edition, October 2009. URL http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf. Cited September 27, 2012. 34 pages.

U.S. Director of National Intelligence. *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, Covering 1 January to 31 December 2011*. The Director of National Intelligence, web edition, February 2012. URL http://www.fas.org/irp/threat/wmd-acq2011.pdf. Cited August 15, 2012.

U.S. Nuclear Regulatory Commission. *Fact Sheet: Uranium Enrichment*. United States Nuclear Regulatory Commission, web edition, October 2011. URL http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/enrichment.pdf. Cited August 20, 2012. 3 pages.

Vacon Group. VACON NXS. Web document, October 1, 2010. URL http://www.flickr.com/photos/vacon-drives/5040586815/in/photostream. Cited October 23, 2012.

Vacon Plc. *Vacon AC drives for high speed applications*, web edition, February 14, 2007. URL http://www.hawaco.com.vn/images/File/High%20Speed%20Applications.pdf. Cited September 13, 2012. 2 pages.

Vacon Plc. *Vacon High Speed Application manual*, ASFIFF12V302 edition, May 14, 2010a. 65 pages.

Vacon Plc. Stuxnet does not infect Vacon AC drives. Web document, November 17, 2010b. URL http://www.vacon.com/Default.aspx?id=480277. Cited August 13, 2012.

Vacon Plc. *AC Drive Product Catalog, North American version*, web edition, May 2012. URL http://www.vacon.com/Default.aspx?id=450403&FileView=468932. Cited August 30, 2012. 115 pages.

Veltman, A., Pulle, D., and de Doncker, R. *Fundamentals of Electrical Drives*. Springer, Heidelberg, 2007. 346 pages.

Walker, D. Saudi oil company back online after cyber sabotage attempt. *SC Magazine*, web edition, August 27, 2012. URL http://www.scmagazine.com/saudi-oil-company-back-online-after-cyber-sabotage-attempt/article/256313/. Cited November 21, 2012.

Waters, D. A. *The American Gas Centrifuge Past, Present, and Future*. USEC Inc., web edition, October 13, 2003. URL http://www.osti.gov/energycitations/purl.cover.jsp?purl=/912770-dBuasR/912770.PDF. Cited September 26, 2012. 10 pages.

Wikimedia Commons. Diagram illustrating the basic principle behind a Zippe-type gas centrifuge enrichment of uranium. Web document, October 8, 2006. URL http://commons.wikimedia.org/wiki/File:Zippe-type_gas_centrifuge.svg. Cited October 23, 2012.

Winter, J. Infamous international hacking group LulzSec brought down by own leader. *FOX News Network*, web document, March 6, 2012. URL http://www.foxnews.com/tech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/. Cited October 15, 2012.

Wireshark Foundation. About Wireshark. Web document, 2008. URL http://www.wireshark.org/about.html. Cited January 3, 2013.

Wireshark Foundation. Download Wireshark. Web document, 2012a. URL http://www.wireshark.org/download.html. Cited January 3, 2013.

Wireshark Foundation. Wireshark 1.8.4 and 1.6.12 released. Web document, November 28, 2012b. URL http://www.wireshark.org/news/20121128.html. Cited January 3, 2013.

Wireshark Wiki. USB capture setup. Web document, November 4, 2011. URL http://wiki.wireshark.org/CaptureSetup/USB. Cited December 30, 2012.

Wood, H. G., Glaser, A., and Kemp, R. S. The gas centrifuge and nuclear weapons proliferation. *Physics Today*, web edition, 61(9):40–45, September 2008. URL http://dx.doi.org/10.1063/1.2982121. Cited January 25, 2013.

Yaskawa America, Inc. *Decanter Centrifuge Application Overview*, web edition, December 8, 2010. URL http://www.yaskawa.com/site/dmdrive.nsf/(DocID)/AHUG-6LZUG7/$file/AO.AFD.65.pdf. Cited August 16, 2012. 3 pages.

Zetter, K. How digital detectives deciphered Stuxnet, the most menacing malware in history. *Wired*, web edition, July 11, 2011. URL http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/. Cited August 13, 2012.

A Safety Functions

This appendix describes the standardized safety functions applicable to AC drives (Table A1). However, not all of them are implemented in real AC drive products. They are presented here to provide information regarding what options are available for power drive systems suitable for safety-related applications (PDS(SR)) by the standards.

Table A1: Safety functions described by International Electrotechnical Commission [2007, p. 16–18] (IEC) in the international standard IEC 61800-5-2 *Adjustable speed electrical power drive systems—Part 5–2: Safety requirements—Functional*

Safety Function	Description
	Stopping functions
Safe torque off (STO)	Energy capable of generating torque is not provided to the motor by the PDS(SR). STO corresponds to "an controlled stop in accordance with stop category 0 of IEC 60204-1."
Safe stop 1 (SS1)	Motor is decelerated, possibly with a limited rate, and after reaching a specified speed limit or time delay the STO function is initiated.
Safe stop 2 (SS2)	Same as the SS1 above, except that safe operating stop (SOS) is initiated instead of STO.
	Other safety functions
Safe operating stop (SOS)	The motor is prevented from deviating from the stopped position more than a specified amount, by providing energy to the motor for resisting imposing forces without external (e.g. mechanical) brakes.
Safely-limited acceleration (SLA)	The motor is prevented from exceeding the specified acceleration limit.
Safe acceleration range (SAR)	Acceleration and/or deceleration of the motor is kept within specified limits.
Safely-limited speed (SLS)	The motor is prevented from exceeding the specified speed limit.
Safe speed range (SSR)	The motor speed is kept within specified limits.
Safely-limited torque (SLT)	The motor is prevented from exceeding the specified torque.
Safe torque range (STR)	The motor torque is kept within the specified limits.
Safely-limited position (SLP)	The motor shaft is prevented from exceeding the specified position limit(s).
Safely-limited increment (SLI)	The motor shaft is prevented from exceeding the specified limit of "position increment", by stopping the motor after the traveling required for the increment.
Safe direction (SDI)	The motor shaft is prevented from moving in the specified direction.
Safe motor temperature (SMT)	The motor temperature is prevented from exceeding a specified upper limit.
Safe brake control (SBC)	A safe output signal is provided for controlling an external brake.
Safe cam (SCA)	A safe output signal is provided to indicate that the motor shaft position is within a specified range.
Safe speed monitor (SSM)	A safe output signal is provided to indicate that the motor speed is below a specified limit.

B Version Information of the Compared AC Drives

This appendix contains relevant hardware type and software version information of the AC drives compared in this thesis. The data (Table B1) is presented as stated on stickers on the drives or as reported by the PC software by the manufacturers.

Table B1: Version information of the different components of the AC drives compared in this thesis, presented as stated by the manufacturers

ABB ACS880-01	
Whole drive	ACS880-01-02A4-3+K473+L517+R700, Frame R1, Assembled in Finland, Firmware version: AINF0 v1.30
Power unit	SBU-A1
Control unit	ZCU-11
Memory unit	ZMU-01
Control panel	ACS-AP-I, SW V3.10
PC tool	Drive Composer Pro v. 1.2.1.0 © ABB Oy Drives 2012
Safety option	FSO-11 Safety functions module, Type: R6030, Rev: F
Ethernet option	FENA-11 Ethernet adapter, 51.32 FBA comm SW ver: 0x0072, 51.33 FBA appl SW ver: 0x0255
Encoder option	FEN-11 Absolute encoder interface
Rockwell Allen-Bradley PowerFlex 755	
Whole drive	Cat No: 20G11 N**C** 2P1 JA0NNNNN, Series: A, Product Revision: 5.001, Product of USA FAC 1100
Control panel	20-HIM-A6, Series A, Enhanced HIM, Firmware: V 2.002, Product of Mexico 1150
PC tool	DriveExplorer, Version: 6.04.99 — Full, Copyright © 2012 Rockwell Automation Technologies, Inc.
Main Control	Firmware Revision 5.001, Hardware Change Number 02
Power Board	Firmware Revision 1.001, Hardware Change Number 01
Encoder option	20-750-USB-1 Universal Fdbk *UFB-1, Firmware Revision: 1.015, Series: A
Safety option	20-750-S1 Safe Speed Montr *S1, Firmware Revision: 1.007, Series: A
EtherNet/IP	Revision: 1.001
DeviceLogix	Revision: 2.004
USB to DPI	1203-USB, Revision: 1.004
Siemens SINAMICS S110	
Power Module	PM340, 6SL3210-1SE12-2UA0, Version: C02, Made in United Kingdom
Control Unit	CU305 PN, SINAMICS Control Unit, (1P)6SL3040-0JA01-0AA0, Version: B, Made in Germany
Memory Card	6SL3054-4EB00-0AA0, SINAMICS S110
Operator Panel	B0P20, Basic Operator Panel, 6SL3055-0AA00-4BA0, Version: A D
PC tool	Drive ES — Starter V4.3.1.2, Copyright © 1999-2012, Siemens AG
Firmware version	4.4.0.12

In addition to the AC drives, the test setup included other equipment also. Details regarding them are listed in Table B2.

Table B2: Technical details of the other equipment used in the test setup

USB to RS-232/-485 adapter	Moxa UPort 1450l, Rev.: 1.2 , Moxa Technologies Co., Ltd., Made in Taiwan
Motor used with ACS880	ABB Motor 3 CI.F IP55 IEC34, M2AA080B 3GAA082002-ASA, 380-420 Y, 50 Hz, 1420 min^{-1}, 0.75 kW, 2.0 A, cosφ 0.74
Motor used with PowerFlex 755	ABB QAL56M4B, I_N=0.6 A, U_N=230 V, f_N=50 Hz, n_N=1330 rpm, P_N=0.1 kW, cosφ=0.5 kW
Motor used with S110	ABB M2VA63B4 3GVA062142-ASC, I_N=1.2 A, U_N=230 V, f_N=50 Hz, n_N=1360 rpm, P_N=0.18 kW, cosφ=0.71 kW, T_N=0.82 Nm

All of the software tools used in this thesis are summarized in Table B3 along with the exact versions used. Also operating systems are listed, thus specifying the whole (virtual) software environment used.

Table B3: Summary of the PC software and their versions used in this thesis

Software	Version(s)
Host OS: Windows 7 Enterprise	6.1, build 7601, service pack 1 (SP1) 32-bit
VirtualBox	4.1.10, 4.1.18, 4.1.20, and 4.2.6
Guest OS: Windows 7 Enterprise	6.1, build 7601, SP1 32-bit
VM network settings	Bridged Adapter, Intel(R) 82579LM Gigabit Network Connection, Adapter Type: Intel PRO/100 MT Desktop (82540EM), Promiscuous Mode: Allow All
ABB Drive Composer	Pro 1.2.1.0
Rockwell DriveExplorer	Full 6.04.99
Siemens STARTER	4.3.1.2
Wireshark	1.8.3 with WinPcap version 4.1.2
Guest OS: BackTrack Linux	5 R3 32-bit with GNOME (ISO-image)
VM network settings	Same as above (for Windows 7)
Nmap	6.01
Zenmap	6.01
Metasploit	4.5.0-dev [core: 4.5 api:1.0]
Armitage	1.44
THC-Hydra	7.3
Wireshark	1.8.1 with libpcap 1.0.0

C Security Checklist for AC Drives for Decanters

This appendix contains the security checklist (Table C1) which can be used as a guide when configuring AC drives for decanter centrifuge applications with Ethernet-based fieldbus connectivity. The security checklist consists of separate actions in the order of execution from top to bottom, according to the defense-in-depth strategy. Following the checklist, the configuration of AC drives should be optimal from the cybersecurity point of view.

Table C1: Checklist. Note! To be completed *before* connecting the decanter centrifuge to a plant-wide network/fieldbus.

Action	X
Initial Preparations	
Make sure the AC drives are physically inaccessible for unauthorized persons (e.g. locked cabinets, etc.)	
Confirm that the engineering workstation is free from malware and has proper security solutions in place, updated, and working, preferably based on application whitelisting for maximum security	
AC Drive Commissioning/Configuration	
Configure private IP addresses (for example 10.0.0.1 and 10.0.0.2) for the AC drives according to site network policy	
Configure motor data and possible encoders	
Configure limit parameters for speed, torque, acceleration, etc.	
With safety option: Configure safely-limited speed (SLS) as constantly enabled with the speed limit below the first rotor critical speed	
With safety option: Verify that the SLS function actually works	
With safety option: Change the safety password from the (factory) default using as complicated password as possible with maximum length	
Configure fieldbus communication	
Enable write masks or similar function (if available) for remote connections (fieldbus) if remote parameter writes are not required	
Disable web and other interfaces of AC drives if not required	
Network Configuration	
Make sure network segmentation is in order by strict firewall rules defaulting to “deny all” rule	
Enforce strict policies on computers allowed within the control network, preferably requiring application whitelisting	
Filter (deny) all IPv6 traffic to/from the AC drives	
Configure industrial protocol monitor at least for the control (fieldbus) network	
Configure security information and event management (SIEM) system for the whole network	