UNIVERSITY OF TWENTE.

DETECTING CYBER ATTACKS IN CRITICAL INFRASTRUCTURES

Dina Hadžiosmanović
DISTRIBUTED AND EMBEDDED SECURITY

Information Technology for Resilient Societies,
October 2011

ARE THE CYBER ATTACKS HAPPENING?

UNIVERSITY OF TWENTE.

CYBER ATTACKS IN CRITICAL INFRASTRUCTURES

"UNINTENTIONAL INCIDENTS"

- **CSX Train Signalling system, USA – 2003**
  - *Sobig* virus shut down signalling, dispatching, etc.
- **Davis Besse nuclear power plant – 2003**
  - *Slammer* virus disabeled plant monitoring system
- **Zotob worm – 2005**
  - work disruptions in DaimlerChrysler U.S., Boeing,...
- ...

UNIVERSITY OF TWENTE.

CYBER ATTACKS FOR CRITICAL INFRASTRUCTURES

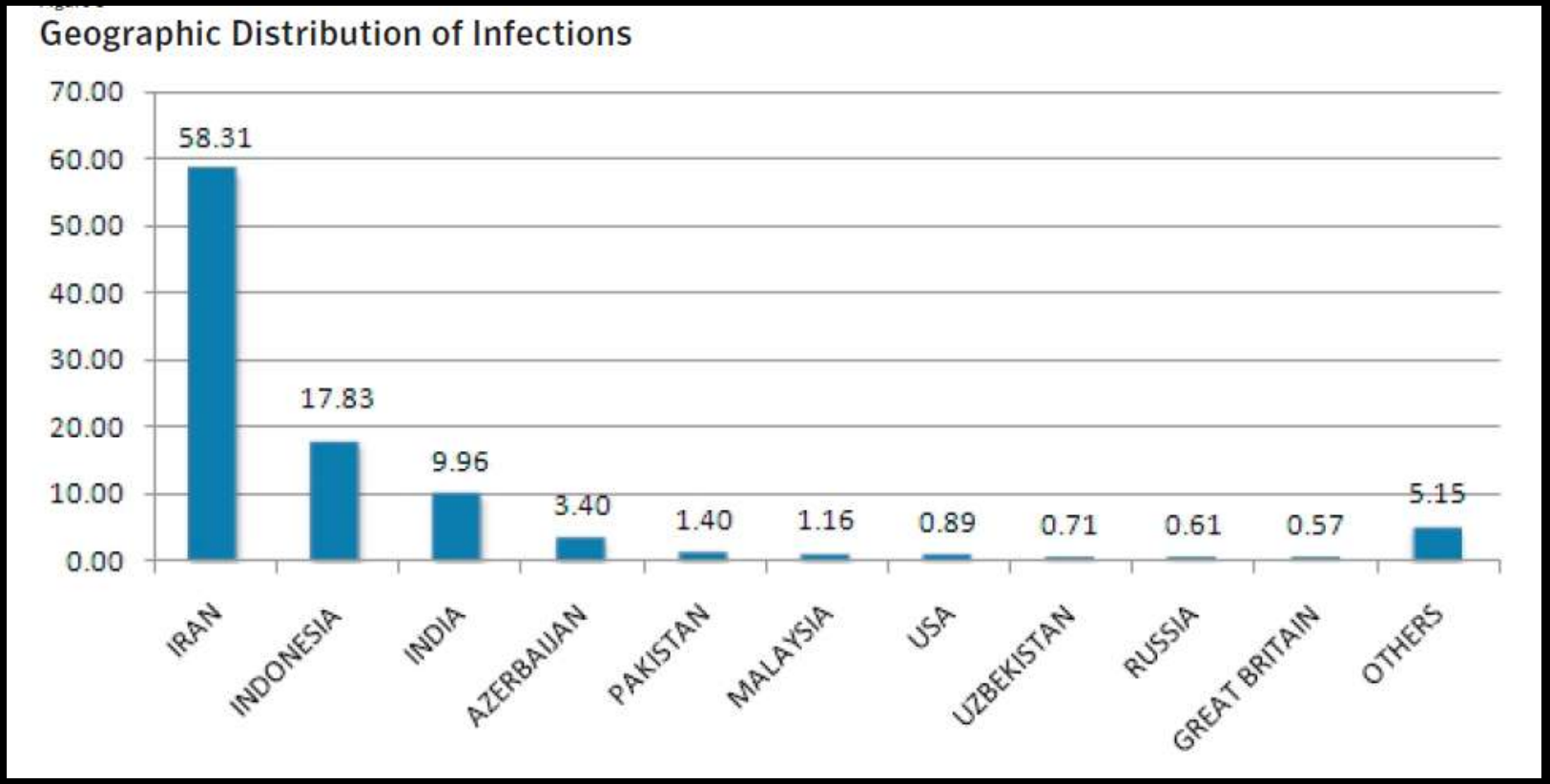
"INTENTIONAL INCIDENTS"

- **Worcester Air Traffic Communications, USA – 1997**
  - a teenager disabled part of the public telephone network on a local airport;
- **Maroochy Shire Sewage Spill, Australia - 2000**
  - a former employee uses personal credentials to disrupt plant work ;
- **L. A. Traffic light system, USA - 2007**
  - Engineers reprogrammed traffic lights to cause traffic jam
- **STUXNET - 2010**
  - A complex virus targeted at disrupting the work of PLC in the targeted environment
- ...

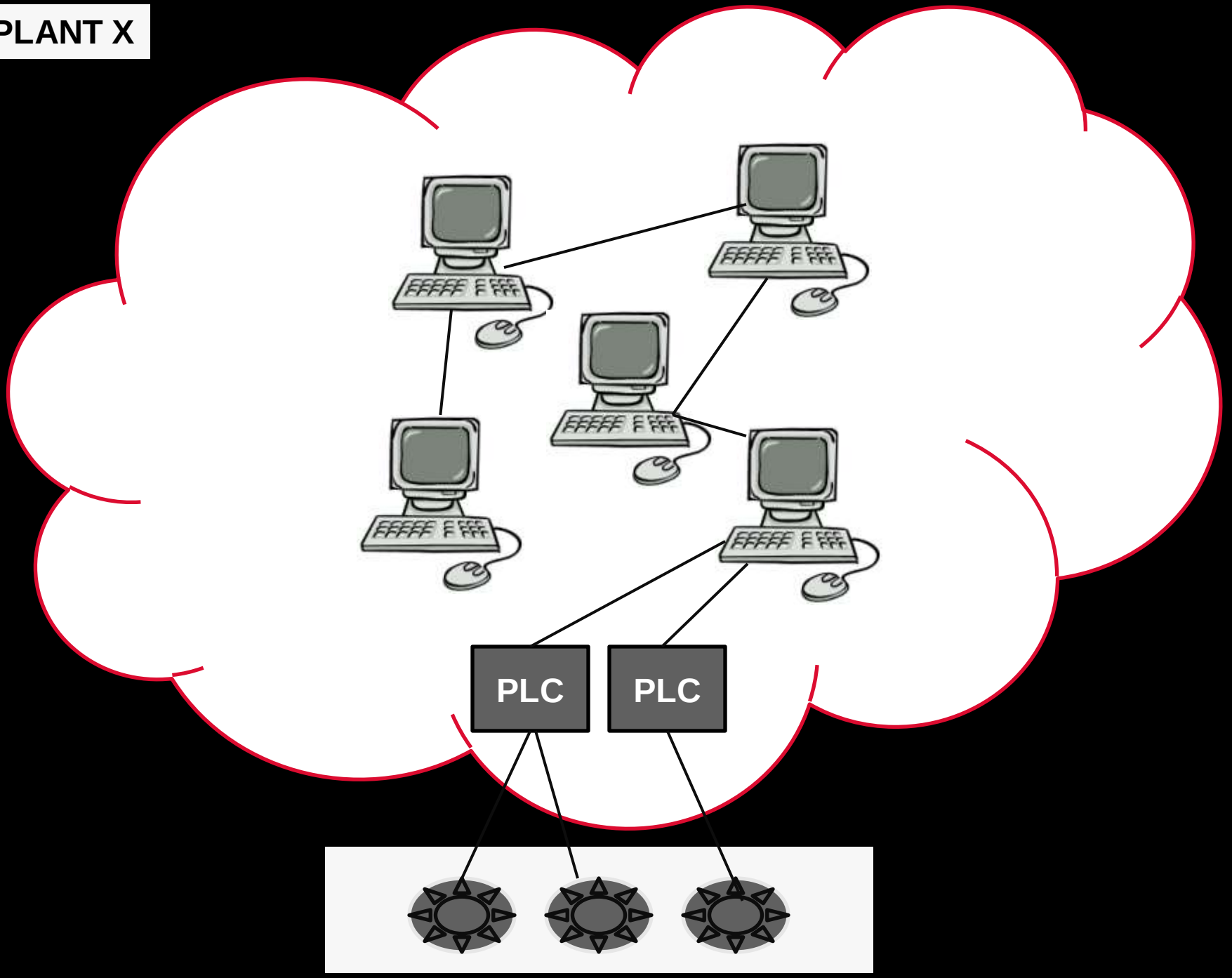
STUXNET

UNIVERSITY OF TWENTE.

- Infected approximately 100 000 hosts
- Aimed as sabotaging motors in uranium-enrichment plant in Iran



PLANT X



PLANT X

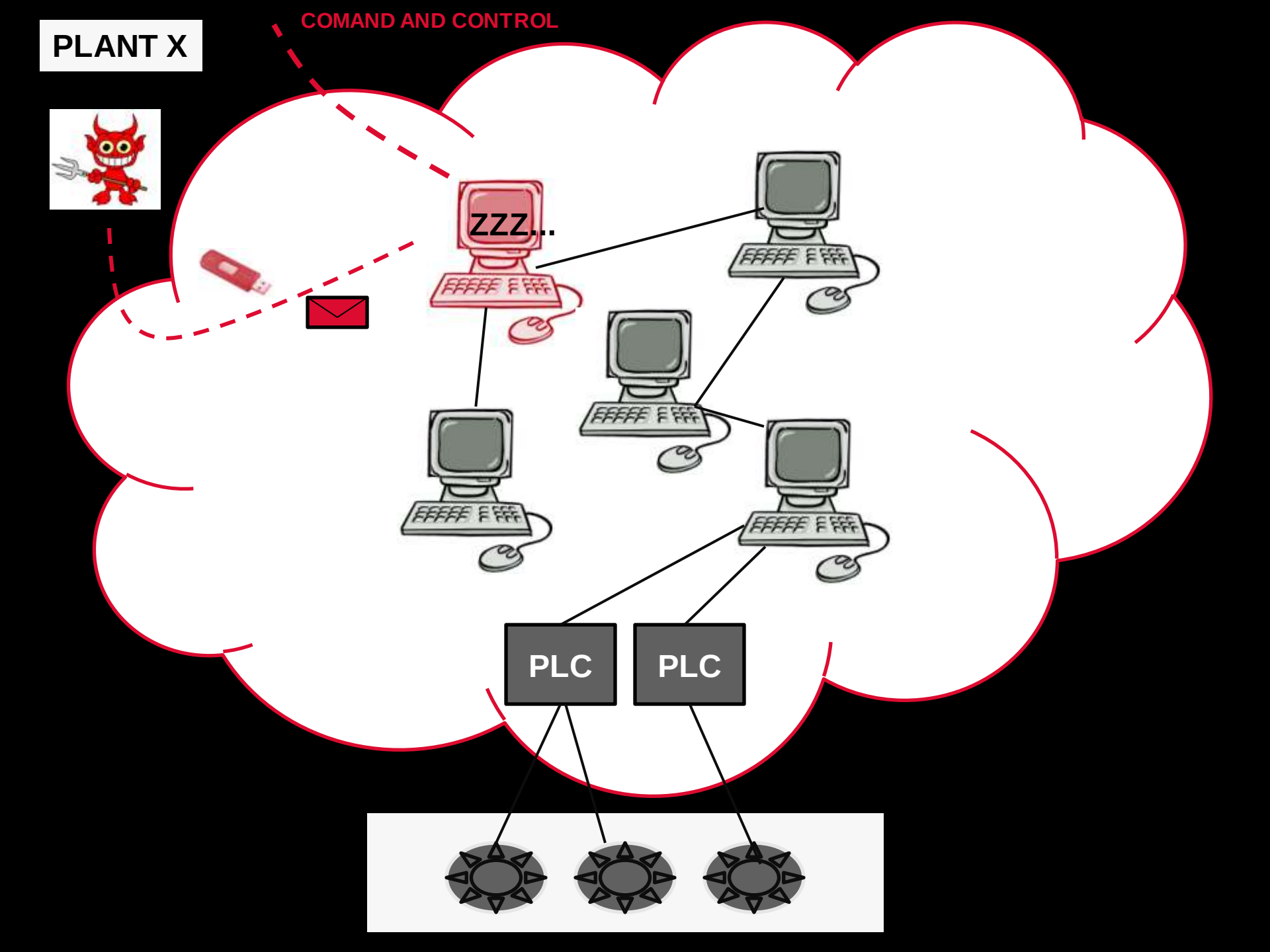
Are you a PLC

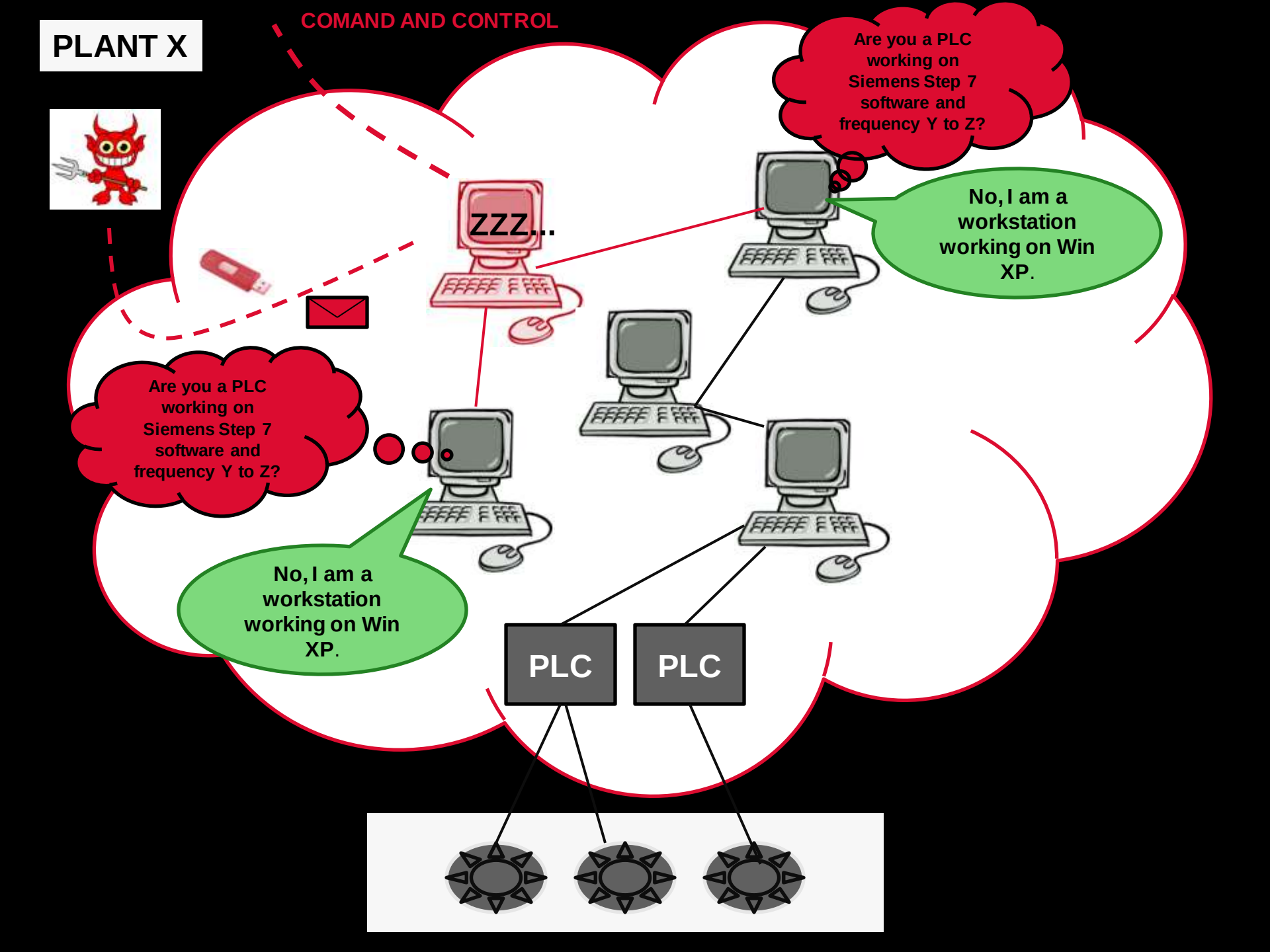
No, I am a workstation working on Win XP.

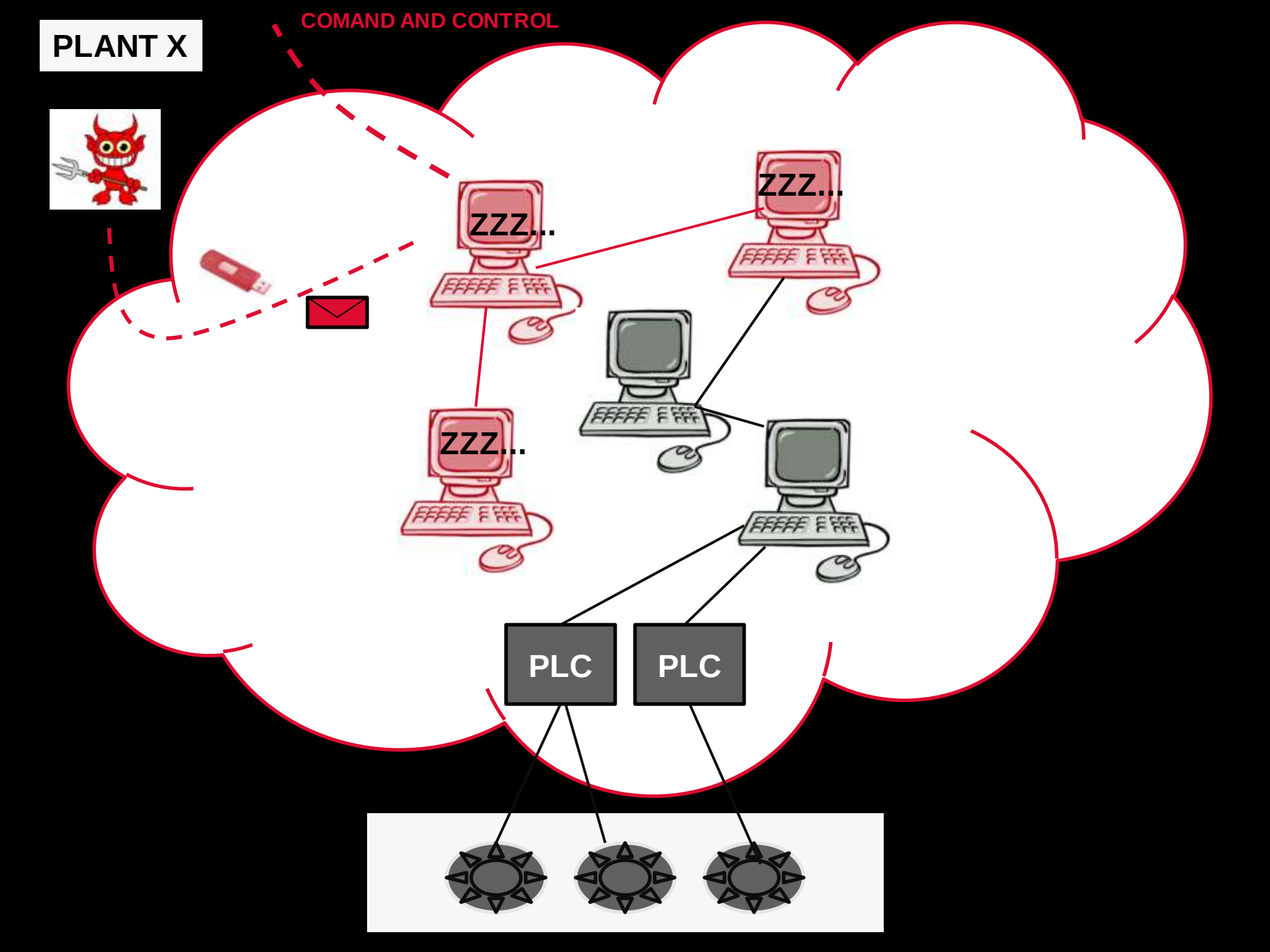
OK, then I sleep now.

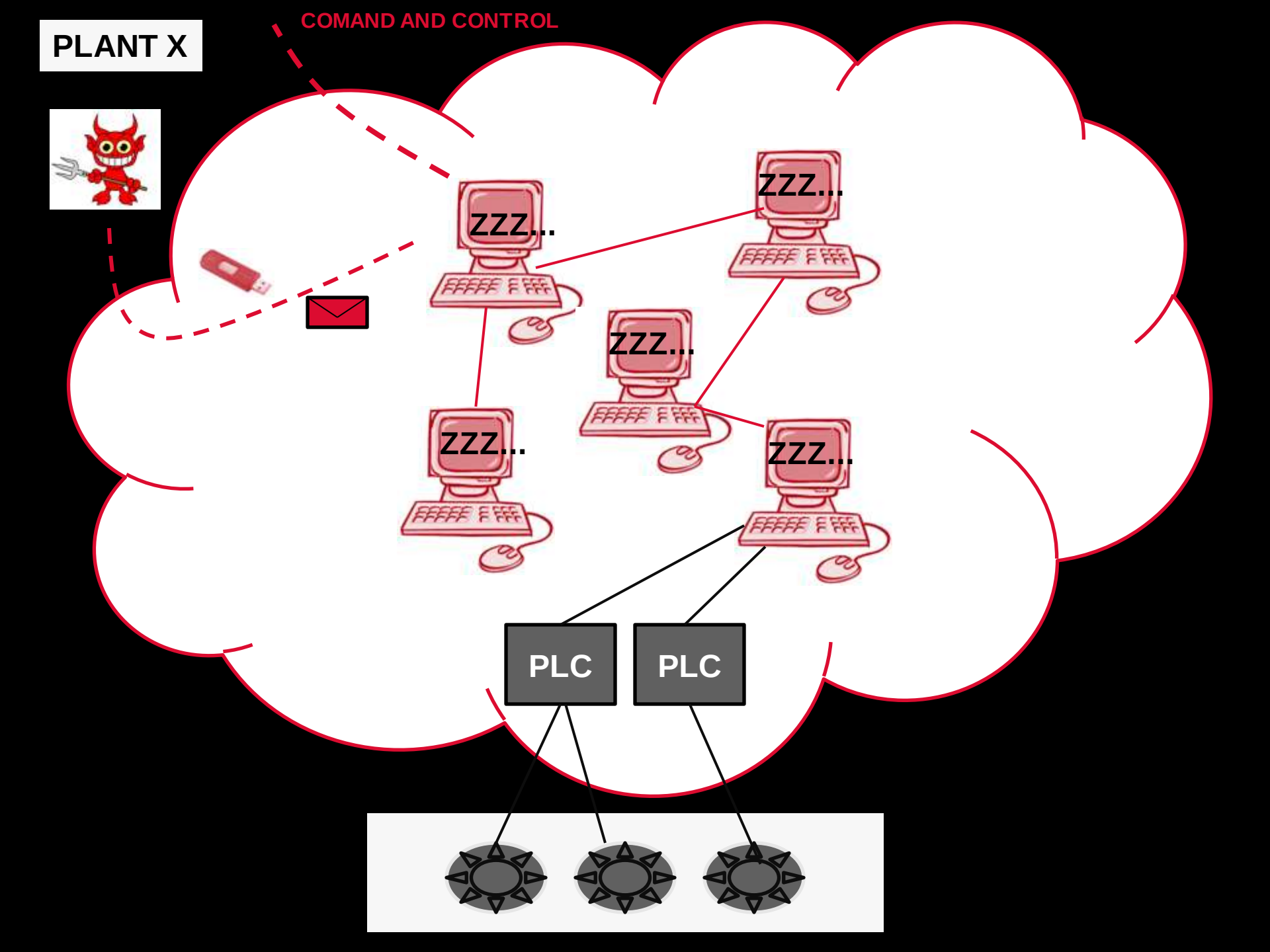
PLC

PLC


PLANT X
COMAND AND CONTROL
ZZZ...
PLC
PLC


PLANT X
COMAND AND CONTROL
Are you a PLC working on Siemens Step 7 software and frequency Y to Z?
No, I am a workstation working on Win XP.
ZZZ...
Are you a PLC working on Siemens Step 7 software and frequency Y to Z?
No, I am a workstation working on Win XP.
PLC
PLC


PLANT X
COMAND AND CONTROL
ZZZ...
ZZZ...
ZZZ...
PLC
PLC


PLANT X
COMAND AND CONTROL
ZZZ...
ZZZ...
ZZZ...
ZZZ...
ZZZ...
PLC
PLC

PLANT X

COMAND AND CONTROL

ZZZ...

ZZZ...

ZZZ...

ZZZ...

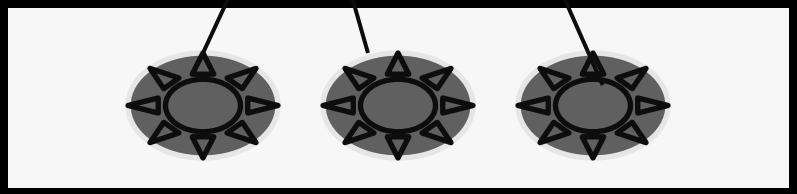
ZZZ...

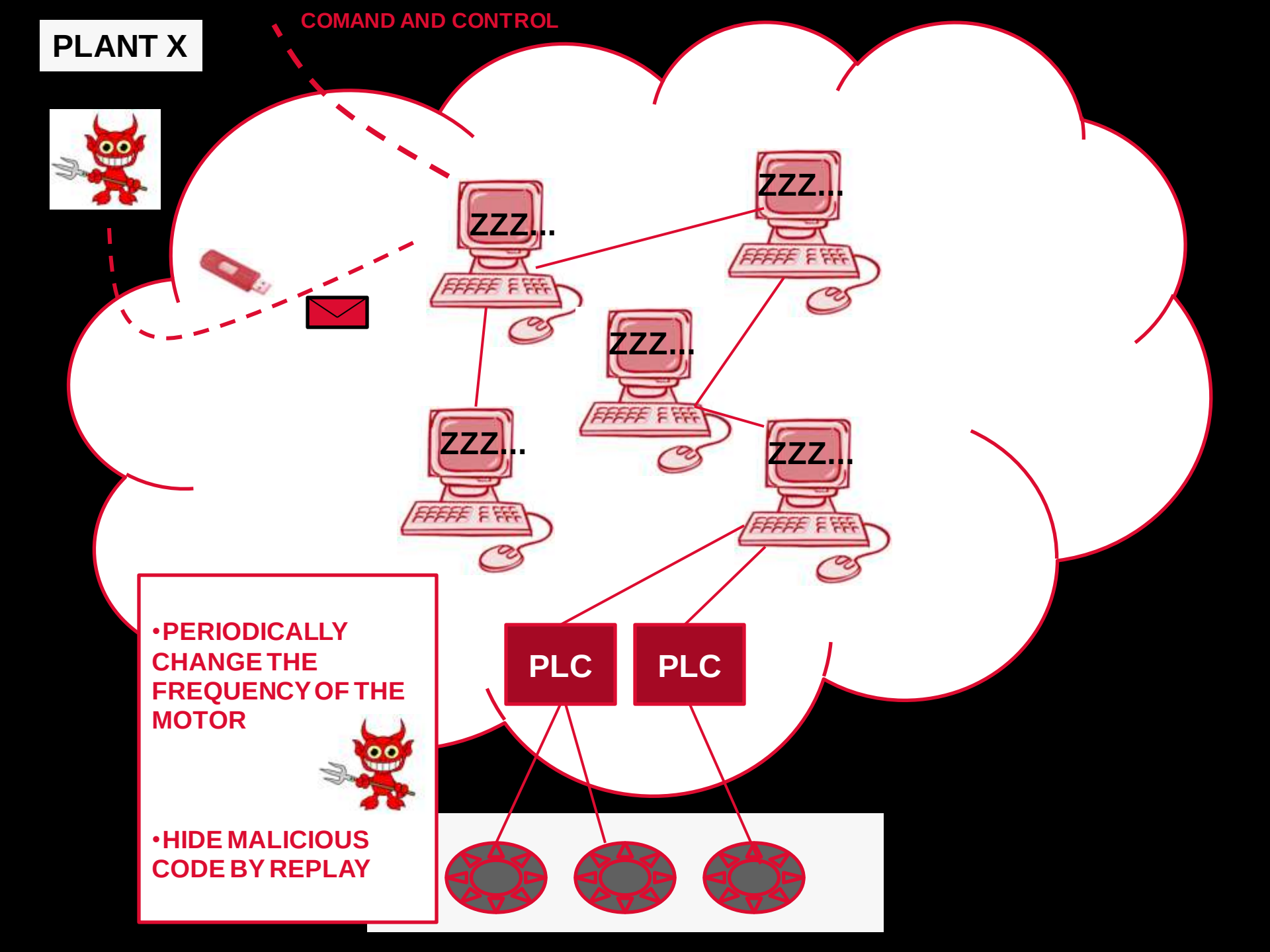
Are you a PLC working on Siemens Step 7 software and frequency Y to Z?

PLC

PLC

YES I am!




PLANT X
COMAND AND CONTROL
ZZZ...
ZZZ...
ZZZ...
ZZZ...
ZZZ...
PLC
PLC
•PERIODICALLY CHANGE THE FREQUENCY OF THE MOTOR
•HIDE MALICIOUS CODE BY REPLAY

UNIVERSITY OF TWENTE.

STUXNET FACTS

- Showed complex behaviour, multiple modes of spreading
- Represents a targeted attack
- The development required process-specific knowledge
- Expensive: used 4 critical, previously undisclosed vulnerabilities
- Has reached the target?

WILL THE NEXT STUXNET BE DETECTED BEFORE HE REACHES HIS TARGET?

UNIVERSITY OF TWENTE.

CRITICAL INFRASTRUCTURES
IN THE CONTEXT OF COMPUTER SECURITY

FEATURES	PROBLEMS
• "security through obscurity"	• outdated
• availability requirement	• slow changes and updates
• interconnected and dependable	• vulnerable as the weakest link
	• reachable to cyber attackers
• important for the society	• an attractive target

The Washington Times

Hacker group threatens industrial computer systems

By Shaun Waterman - The Washington Times — Monday, October 17, 2011

STORY TOPICS

Technology_Internet
Department Of Homeland Security
National Cybersecurity And Communications Integration Center

QUESTION OF THE DAY

Do you think Herman Cain's '9-9-9' tax-reform proposal is a viable plan?

The Department of Homeland Security (DHS) is warning that hackers from the loose online protest collective called Anonymous have threatened attacks against the computer systems that run factories, power stations, chemical plants, and water and sewage facilities.

"While Anonymous recently expressed intent to target [industrial control software], they have not demonstrated a capability to inflict damage to these systems," reads a leaked bulletin from from the department's National Cybersecurity and Communications Integration Center.

DHS did not immediately respond to a request for comment.

Industrial control software (ICS) systems, also known as Supervisory Control And Data Acquisition (SCADA) systems, are considered among the most dangerous targets for hackers because successful attacks could damage or destroy the industrial equipment they control — blowing up power generators, releasing clouds of dangerous chemicals or polluting water supplies.

http://aluigi.org/adv/igss_7-adv.txt
http://aluigi.org/adv/igss_8-adv.txt

FEATURED


'Fast & Furious': How a botched operation spawned fatal results
By Jerry Seper - The Washington Times


'9-9-9' tax plan raising Cain, doubts
By Seth McLaughlin - The Washington Times


Consumer electronics chief says Obama regulators lack business experience
By Tim Devaney - The Washington Times

COMMENTARY

WOLF: Liberalism's unwashed last stand
By Dr. Milton R. Wolf
The hippie-critical new faces of the Democratic Party

CHIN: Obama's infrastructure bank won't create real jobs

WILL THE NEXT STUXNET BE DETECTED BEFORE HE REACHES HIS TARGET?

HARDLY.

WHAT CAN BE DONE?

UNIVERSITY OF TWENTE.

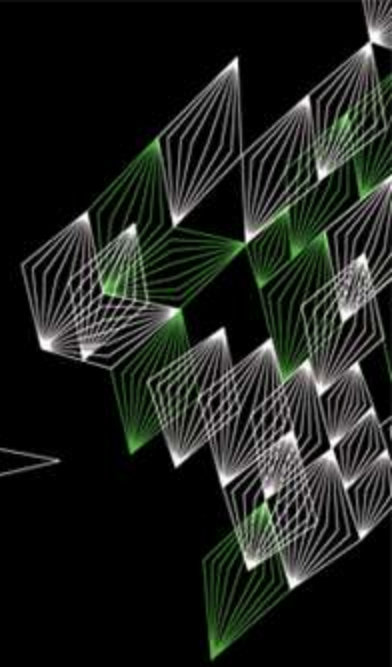
1. PROMOTE AND PRACTICE GENERAL SECURITY MEASURES

- raise awareness, improve password policy, access control, status monitoring, virus protection, advanced network administration and segmentation, etc.

2. SMART MEASURES FOR SMART ATTACKS

- improve process monitoring
  - Hadziosmanovic, Dina and Bolzoni, Damiano and Hartel, Pieter and Etalle, Sandro (2011) *MELISSA: Towards Undesirable User Actions in Critical Infrastructures,* In: European Conference on Computer Network Defense, EC2ND 2011, 6-8 Sept 2011, Gothenburg, Sweden.
- understand threats
  - Hadziosmanovic, Dina and Bolzoni, Damiano and Hartel, Pieter (2010) *Towards securing SCADA systems against process-related threats,* Technical Report TR-CTIT-10-35, CTIT, University of Twente, ISSN 13813625 *doc.utwente.nl/74077/1/Hadziosmanovic2.pdf*
- develop process/protocol aware techniques for detecting intrusions

UNIVERSITY OF TWENTE.



THANK YOU!