The Power Plant  
Electrical power starts at the power plant. In almost all cases, the power plant consists of a **spinning electrical generator**.

Transmission Substation  
The three-phase power leaves the generator and enters a **transmission substation** at the power plant. This substation uses large transformers to convert the generator's [voltage](http://science.howstuffworks.com/question501.htm) (which is at the thousands of volts level) up to extremely high voltages for long-distance transmission on the transmission grid.

The Distribution Grid  
For power to be useful in a home or business, it comes off the transmission grid and is **stepped-down** to the distribution grid. This may happen in several phases. The place where the conversion from "transmission" to "distribution" occurs is in a **power substation**. A power substation typically does two or three things:

* It has transformers that step transmission voltages (in the tens or hundreds of thousands of volts range) down to distribution voltages (typically less than 10,000 volts).
* It has a "bus" that can split the distribution power off in multiple directions.
* It often has circuit breakers and switches so that the substation can be disconnected from the transmission grid or separate distribution lines can be disconnected from the substation when necessary.
* the background, the incident, the aftermath
* why it is interesting/important
* what was wrong in: securing information (before the incident), assessing and predicting the risk, incident response, handling the consequences, etc.

Introduction:

Ukraine has 24 regions, each divided into between 11 and 27 provinces, with a different power distribution company serving each region.

It was 3:30 p.m. last December 23rd, Prykarpattyaoblenergo control center, Ivano-Frankivsk region of Western Ukraine, the cursor on one of the operator’s computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline.

A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive.

All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another, eventually taking about 30 substations offline and leaving more than 230,000 residents in the dark.

Highlight:

The hacker also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.

Timeline:

Reconnaissance phase:

Getting into the Network:

Last Spring, the attackers delivered spear-phishing email with a malicious Word document attached targeting IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine.

When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3 infected their machines and opened a backdoor to the hackers.

The initial intrusion got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid.

Getting into SCADA:

Over many months of exploring and mapping the networks, they got access to the Windows Domain Controllers, where user accounts for networks are managed.

They harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network.

Reconfiguring the UPS:

They reconfigured the uninterruptible power supply, or UPS, responsible for providing backup power to two of the control centers.

Replacing legitimate firmware:

They wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations resulting in blocking operators from sending remote commands to re-close breakers once a blackout occurred.

INCIDENT:

Sometime around 3:30 p.m. on December 23 they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured.

Then they began to open breakers.

They launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage.

As the attackers opened up breakers and took a string of substations off the grid, they used their malicious firmware to render the converters thereafter inoperable and unrecoverable, unable to receive commands.

After they had completed all of this, they then used a logic bomb that launched malware called KillDisk automatically about 90 minutes into the attack to wipe files from operator stations to render them inoperable as well.

This would have been around 5 p.m., the same time that Prykarpattyaoblenergo posted a note to its web site acknowledging for the power outage.

Half an hour later,the company then posted a second note to customers saying the cause of the outage was hackers.

AfterMath:

The power wasn’t out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers are still not fully operational. The power is on, but workers still have to control the breakers manually.

Their security weakness:

US experts say the control systems in Ukraine were surprisingly more secure than some in the US, since they were well-segmented from the control center business networks with robust firewalls.

But in the end they still weren’t secure enough—workers logging remotely into the SCADA network, the Supervisory Control and Data Acquisition network that controlled the grid, weren’t required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers.

What was Wrong and What can be done:

The employees did not have awareness about spear-phishing.

It should be common practice to train the employees about phishing, providing segregate networks, and having white-listing technology in place, rather than just anti-virus software.

The networks does not support constant monitoring protocols that recognize the anomalies which indicate potentially threatening behavior because "if a misconfiguration is made by accident, or malicious code is knocking at the door of a network, protection strategies of this kind can significantly reduce the risk of system outages through cyber attacks".

http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/