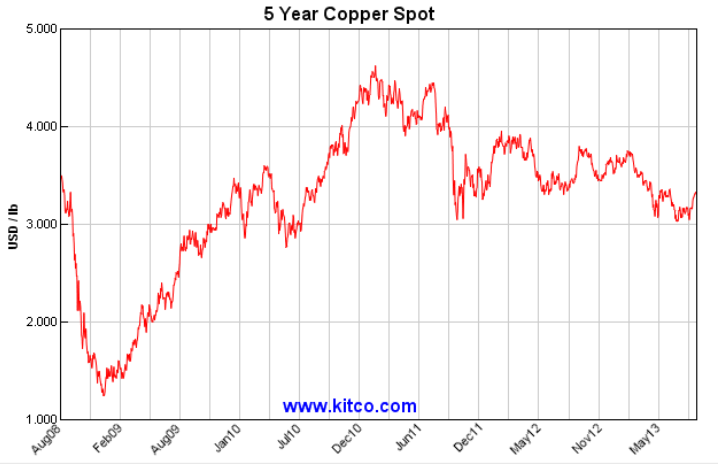
Stop Copper Theft

How Video Analytics are Helping Electrical Utilities Proactively Stop Copper Theft

Cause: A Perfect Storm

Metal thefts, particularly copper, have a direct relationship with the price of copper on the open market. Throughout the last ten years there have been a series of events that have driven the price of copper approximately six times the price of what it was in the previous decade. After a series of supply spikes in 2003-2006 that included the collapse of the Grasberg copper mine in Indonesia and multiple worker strikes in the El Abra mine in Chile, the price continued to climb. At this same time, China became the largest consumer of the four key base metals. In early 2006, copper rose to $3.00 per pound and copper production actually fell below the rate of copper consumption. Prices continued to hold between $3.00-$4.00 throughout 2006, 2007 and the first half of 2008. At prices north of $3.00 copper theft incidents are prevalent. The global market crisis in the fall of 2008 crashed the price of copper to 1990's levels and reported copper thefts dwindled for the later part of 2008 and first half of 2009. In October of 2009, prices crept back up as the market continued to rebound, maxing out at more than $4.50 per pound January of 2011. Prices have held steady between $3.00-$4.00 per pound from December of 2011 to May of 2013 (time to press). Copper is the major form of metal fueling the $65 Billion U.S. scrap-recycling industry. The annual cost of copper theft in the United States is currently estimated at $1 Billion per year.



Effect: Copper Theft

Theft of copper wiring from electrical utility sites creates more the 7,500 hours of downtime which costs the industry more than $60 million annually. There are two key reasons why electric utility substations are the number one target for copper theft in the United States. First is that copper is the main component for distribution and grounding of electrical power and therefore is available in abundant supplies in even small to medium size substations. Large quantities of copper wiring for grounding and transmission at substations can exceed 2000 ft. The second reason is electric utility substations are often situated in remote locations with little to no security. For many substations, a chain-link fence with barbed-wire edging is the extent of security technology deterring would be thieves. The remote locations often with little security give thieves ample time and opportunity to remove the copper wiring.

Although the quantity and lack of security is attractive to thieves interested in stealing copper, the risk to the Utility companies is far greater than simply the cost of the lost copper wiring. Since the wiring is

used in distribution and grounding, stripping copper wiring out of the substation can easily knock out power to thousands of paying electricity customers. Thieves are not only risking their lives, as many would be thieves have been electrocuted in the process of stealing copper wiring from substations, but they are risking the lives of utility workers sent in to repair the damage. Damage is often thousands of dollars more expensive than the cost of the stolen wire. In many cases, when scrap recycling companies have identified copper wiring as coming from an electrical utility and contacted the authorities, the utilities do not chose to retrieve the stolen property because it is useless for its original purpose.

Another factor that adds to the cost of copper theft for the utility industry is when thieves steal spools of copper from work-sites or storage facilities. These spools can be easy targets because they contain large amounts of copper and the physical danger of stealing them is far less than stripping live copper grounding wire from substations. Although the physical danger may be less, copper spools are typically stored in facilities with higher levels of physical security than utility substations. The risks of getting caught stealing can be greater but so too can the rewards, a large spool of copper can contain 1300 pounds of copper. Utilities often must pay union labor even though they are unable to work when they get onsite and all of their materials have been stolen which adds to the money lost as a result of copper theft.

Reaction: Current Solutions

As the frequency of copper thefts has fluctuated with the price of copper on the world market over the years, so too has the approach to reduce or solve the problem. The two mitigation practices that are generally sited when the copper theft issue is discussed are legislation and improved identification. Legislation focuses on pointed the responsibility of the copper theft epidemic squarely on the shoulders of the scrap metal recycling industry. State and Federal laws require scrap metal recycling facilities to keep records of their patron's identity and vehicle license information for a set period which ranges from 30-60 days before the metal can be converted on the open market. This process which is called "Tag and hold" is designed to give Copper Theft victims ample time to report and investigate the local scrap metal facilities to recover stolen property and prosecute thieves. The goal is that copper thieves would be deterred from the criminal activity because they would be easily caught and prosecuted. These types of programs have led to innovation in identification applications. Utility companies use an adhesive spray over the wire for so-called "micro-tagging" that when applied will read unique microscopic identification numbers on the wire. The major issue with both of these generally sited methods of course is that they are both reactive in nature. The goal of each solution is to deter the criminal activity of stealing copper from electrical substations based on the consequence of being caught and prosecuted. For deterrence to work effectively it requires a rational person to "realize" and care that

there is a consequence to their action. In other words we have to assume that someone willing to risk their life by cutting live ground wires potentially carrying thousands of volts of electricity for a few hundred dollars is thinking rationally for this approach to be considered an effective strategy. As thieves have shown countless times, once the price of copper reaches the $3.00 threshold there is not much deterrent that can stop them from attempting to steal copper. With the lack of deterrent, tag and hold legislation and improved identification tactics become purely reactive tactics to the problem which at best lead to eventual prosecution and or the return of stolen property. The key issue here is that the damage has already been incurred. Power most-likely was already interrupted to paying utility customers, property has been vandalized and damaged, and a dangerous environment has been left behind for utility contractors to come in and clean up the mess.

Video security plays a key role in the fight against copper theft for most Electrical Utility companies. Inexpensive battery-operated cameras with built-in motion detection triggers offer easy-to-install solutions to allow Utility companies to see what is going on at substations from remote locations. Unfortunately the motion-detection is designed that “something has moved” and is prone to false alarms. The key issue with video motion detection is that it is designed to begin recording when any change in the video occurs. Video motion detection cannot differentiate whether wind blowing trees or debris, rain or snow falling, insects flying in the camera or a small animal is causing the event. From this aspect, motion detection is less effective at detecting the security event because it is designed to detect when “something has moved” and therefore does not discriminate what caused the movement. Video-analytics based systems differ from video motion detection by alerting security when “something you care about is happening.” The software is based on machine vision applications that allow users to create detection zones that alert to violations based on the size of objects and the amount of time an object stays in a specific area in the field of view. Software filters are used to ignore noise caused by bugs, wind blowing tree branches or precipitation in the field of view. Where motion-detection offers little discrimination, video analytics are highly-selective in determining what actually triggers a security event. By applying Video Analytics-based security products at utility substations and works facilities, electrical utilities can receive real-time alert notification when copper thieves get within ten feet of the fence line of a substation and continue to receive alerts after the perpetrator has entered the facility. This proactive solution allows utility companies to potentially stop theft, and the other damages associated with theft, before it occurs.

Case Study: Ameren UE

Customer Profile

Ameren provides energy to more than 2.4 million electric and almost 1 million gas customers in Illinois and Missouri. The company generates a net capacity of 16,800 megawatts of electricity with nearly 86,000 miles of electric distribution and transmission and operates more than 21,300 miles of natural gas distribution and transmission mains for a service area that covers about 64,000 square miles. Ameren also operates coal-fired plants, three hydroelectric plants and more than a dozen combustion turbine facilities.

Surveillance Requirements

Video Security is a key component of the overall physical security profile for Ameren. The company operates with multiple monitoring centers where in-house operators view the output of over 1500 security cameras covering all locations. Significant threats include break-in, trespassing, and potential theft of copper wire. Operational security also requires the use of video security to monitor safety requirements at specific generation facilities.

Customer Concerns

Ameren is concerned with real-time detection of perimeter breaches at multiple facilities. They required a system that could provide video verification of security events such as break-ins, trespassing and theft.

Solution

After a thorough market search of products with analytics capabilities, Ameren selected the ARTECO-IVS. They chose the Arteco solution because it offered a scalable system that caters to both Analog and IP camera solutions, advanced analytics capability with minimum set-up time, and a single-platform interface that is easy to learn and user-friendly. The edge server-based architecture of the ARTECO-IVS gives customers, like Ameren, the ability to grow intelligently while using video analytics for real-time detection and as a resource management tool. The system uses rules-based analytics to detect the size, speed, and time of objects within a specified zone of interest. When the rules are broken, the system alerts in real-time, driving video operators attention to the security event taking place. The ARTECO-IVS allows Ameren to effectively manage network and storage resources by only streaming video over the network when significant events to the security profile take place. Recording capacity stored locally at each site is conserved by increasing the frames per second and resolution when security events take place and scaling back video quality when nothing of significance is occurring.

Ameren has deployed ARTECO-7000 PRO series IVS servers on a hybrid mixture of analog and IP-based cameras. The systems are centrally managed with ARTECO-LOGIC VMS from multiple sites. The ARTECO-IVS is used approximately 500 channels of video security throughout Ameren facilities where each camera is tuned to detect and alert to perimeter violations in real-time with minimal false alarms.

What they say about Arteco

"The ARTECO-IVS offers a proactive solution to alert personnel in real-time and continues to be a vital piece of our perimeter security profile." Karen Summers, IT Supervisor, Physical Security – Ameren Services