NEVER OUT OF REACH

Sole UK Distributor for XCMG Access Equipment

GENESIS
EQUIPMENT SALES

CALL OUR TEAM TODAY ON 01933 232 664
OR VISIT WWW.GENESISEQUIPMENTSALES.COM

SCAN HERE TO FIND OUT MORE

BENEFITS ALL ROUND

It is fitting that this feature on radio remote controls coincides with features on loader cranes and spider lifts - two completely different types of equipment but both have been transformed by the adoption of radio remote controls. There is a noticeable trend however for more types of equipment to adopt the technology, which, apart from possible security issues as highlighted in the report on page 56, have enormous benefits.

The operation of machinery via remote controls allows operators to place themselves in the most beneficial position. With the advent of radio remote controls, operators are no longer confined to a stationary control point - the end of a trailing lead, or in a cab, a platform, or at the side of a machine - but are free to move around to gain the best possible view of the load or when manoeuvring the machine or a load in a tight spot.

MORE APPLICATIONS

The continual development in technology and manufacturing has resulted in a massive growth in applications away from the more traditional use on self-erecting tower cranes, loader cranes and aluminium truck cranes, although even in these applications there are improvements and new features being added all the time. One unusual application recently involved a remote controlled 3,500 tonne spreader beam with an automated sling handling system.

Loader crane manufacturer Hiab recently announced a modified version of its new iX.162 HiPro BSS-2, following an order for 400 from UK builders merchants Travis Perkins, with delivery scheduled over the next three years. The crane features the all-new CombiDrive 4 remote controls - the product of Hiab's acquisition of Swedish electro-hydraulic valve bank and control system manufacturer Olsbergs at the end of last year. The new controller has confirmed view sensors which automatically detects operator position, providing improved safety for the operator, customers and members of the public. The crane has also been designed so that the engine can be stopped and restarted from the remote controller, reducing idling emissions and noise.

ULTIMATE REMOTE

But perhaps the ultimate 'remote control' is the Skyline Cockpit - a tower crane teleoperation system that allows the crane to be operated live and remotely from a ground control system. The system located at ground level has many benefits including reducing the time and effort of climbing up to the cab and also allows operators with a fear of heights or mobility issues to take the job. The operator sits in a spacious air conditioned/heated cabin on the ground with all the usual office comforts.

The system uses a peripheral wide-screen display that replicates the panoramic view from the cab, and it is even possible to operate the crane in the dark using a system based on advanced technological developments, Artificial Intelligence and Augmented Reality. The operator can precisely identify where the crane hook is positioned having visual readouts on the screens covering the height, load weight, wind speed, direction and work speed. The system has been marketed by UK tower crane specialist Radius Group which also claims that the Skyline Cockpit can detect any tower crane problems and immediately address them through preventative maintenance.

One unusual application recently involved a remote controlled 3,500 tonne spreader beam with an automated sling handling system

Hiab's new iX.162 HiPro features ... the all-new CombiDrive 4 remote controls

Perhaps the ultimate 'remote control' is the Skyline Cockpit - a tower crane teleoperation system that allows the crane to be operated live and remotely from a ground control system

'REMOTE ONLY'

There has also been a move towards 'remote only' controls on many types of equipment - even boosting the usefulness of products such as the latest generation of tracked carriers. Spider lift manufacturers are increasingly dispensing with traditional fixed controls in the platform but rely on the radio remote controller which clips into a docking system when the operator is controlling the machine from the platform. This allows them to use the controller to manoeuvre the lift from the basket in the traditional way or quickly remove it to use it remotely when moving the machine, positioning in a tight spot or loading.

This move towards 'remote only' has also gained pace with Italian pick & carry crane manufacturers including Manitex Valla which has announced that it will unveil two more all-new pedestrian controlled all-electric pick & carry models - a 16 and an 18 tonne - although it still offers versions with cabs for those who prefer them. Valla had previously announced two smaller radio controlled cranes the 4.6 tonne V46 R and the 13 tonne V130RX. All of the new models will be launched at the upcoming CIS exhibition next month.

The radio remote control Valla V130RX with chassis extended forward

PRODUCT DEVELOPMENT

As already mentioned remote control manufacturers are constantly developing and improving their products. Most recently Cavotec announced the development of a new lightweight control unit for operators working with mobile and tower cranes over extended periods. The company says its MC3100 is lighter and more compact than many other of its current systems and broadens the scope of RRC applications as it includes all the safety features of its other units designed for the oil, gas and mining sectors. One of its main features is the option for users to easily adjust the height and angle of the controller from their belt, essential when the unit is in constant daily use.

The new Cavotec MC3100 RRC unit

SUSTAINABLE CONSUMPTION

The downside of the boom in the use of radio remotes is the growing amount of electronic or 'E' waste. Last November members of the European parliament called for new measures to promote a culture of repair and reuse, along with support for repair and rebuild as well as second hand businesses, by making it easier and cheaper for consumers to have products repaired. Perhaps this will also allow users to have controls repaired and upgraded - with security patches for example - extending the lifespan and reducing electronic waste. ■

HBC-radiomatic Spectrum B

Autec M-Pro

Hiab iX

RAYCO ELECTRONIC SYSTEM LTD

i5000 Series

NEW PRODUCT NEW DESIGN AND USER EXPERIENCE

RaycoWylie new i5000 reaches the highest level of integration with any type of crane and heavy equipment in the industry. The new platform will be available with remote connectivity, enabling to monitor the performance of your equipment no matter where you are

CANADA

+1 418 266 6600 ext 210

UNITED KINGDOM

+44 1424 421 235

RaycoWylie Crane Division

RaycoSyscomak Heavy Equipment Division

JOIN THE CONVOY

The Plant & Hire Aid Alliance is organising another convoy of aid to people in Ukraine on Sunday 15th and Monday the 16th of October. This will be the third humanitarian run the charity has organised and will travel to the Slovakian town of Chminianska Nová Ves, near to the border with Ukraine, where volunteers from Rotary International will distribute the aid via their humanitarian centres in Uzhorrod and Vinnytsia to those affected by the war.

Several members of the aid alliance have already signed up, but others willing to join the convoy with vans, trucks or estate cars are invited to join the convoy. While it will set out from the UK, there is no reason why companies or individuals based in Continental Europe could not meet up and join along the route.

Rotary International is looking for the any of the items below. Even if you are unable to join the excursion you can always participate by sending any of the items to the address below where Ardent is consolidating the donations. They should be sent to Ardent Hire, 289-297 Felixstowe Road, Ipswich, Suffolk, IP3 9BS before the 7th of October.

ITEMS REQUESTED:

- food, camping food, baby food,
- aids for disabled and elderly,
- hygiene items (except sanitisers),
- generators (5kW and more)
- heaters
- candles, torches
- sleeping bags and mats
- thermal clothing, warm socks
- first aid kits
- power banks
- bedding and blankets
- disposable dishes.

Donations should ideally be packed in boxes or in bags and clearly labelled showing the items and quantities. This will help with clearing items through customs. Those planning to travel with the convoy, but struggling to fill vans might be able to top them up with the donations sent in.

If you would like to participate with a van, please contact the Alliance via email at: **hello@aid-alliance.com**

www.hello@aid-alliance.com

HACKING CRANES – A REAL THREAT

In 2019, two pioneers from the cyber technology industry - Federico Maggi and Marco Balduzzi - embarked on a mission to hack crane remote controllers. They travelled through the Lombardi region of Italy and with the permission of the site managers, were able to demonstrate the vulnerability of lifting equipment taking control of the cranes and hoists often within minutes. The results of their research and others are contained within an 82 page report funded and published by Trend Micro Research entitled 'A security analysis of Remote Controllers for Industrial Applications'. Imogen Campion reports

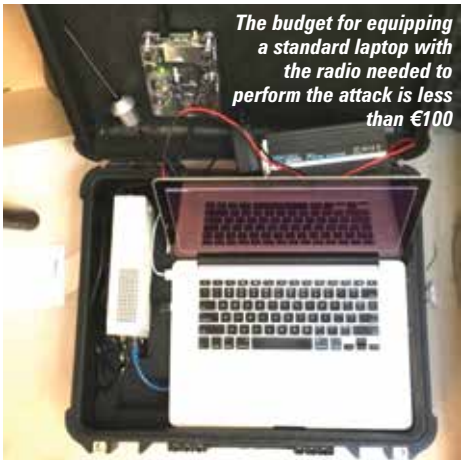
Taking control or hacking cranes involves a simple process using laptops connected to radio frequency (RF) equipment. What Maggi and Balduzzi discovered was that the radio remote control technology used on many, if not most cranes was inherently less secure than that used on the average electric garage door opener and is the weakest link in a safety critical piece of equipment.

In simple language, Maggi and Balduzzi were doing something similar to cloning the transmitter. The vulnerability is not in the lifting equipment but in the communication between the remote controller and the crane. The pair reverse engineered the communications coming from the RF equipment to find ways of copying commands. These should have been in unique formats however, they discovered the command 'data packets' were often transmitted with little or no security which, they say, makes it easy for hackers to replicate using a software-defined radio which scans the bandwidths.

"There is high risk of injury for the operators as well as the cost in damages," says Balduzzi who has been in the cyber security industry for 15 years and warns of the impact if the equipment isn't adequately secured. "It is very easy to attack, it only requires the attacker to sit within the range of coverage of the radio remote controller, usually a few hundred metres, and it is very cheap. The budget for equipping a standard laptop with the radio needed to perform the attack is less that €100."

So far, they are not aware of any recorded attacks, but the point of the exercise was to identify issues before they are targeted by attackers. One of the main goals of conducting the research was to raise awareness of the subject.

Federico Maggi (R) and Marco Balduzzi embarked on a mission to hack crane controllers



The budget for equipping a standard laptop with the radio needed to perform the attack is less than €100

Possible types of attack include:

- **Theft:** Automated ports use industrial RF technology. Due to their sheer size, they are often too large for wired only connections. Attackers can therefore interfere with the lifting operations at say an automated port to hijack or steal in-transit goods. They could also ultimately conduct a larger supply chain attack.
- **Extortion:** The bigger the asset the bigger the risk and the bigger the opportunity. An attacker could cause repeated damage to equipment and demand a ransom to stop.
- **Sabotage**: Incidents that occur at a facility or a construction site can cost months, or even years of programme delays.

CRITICAL CONCERN

A critical concern centres on the use of RF controllers which often feature rudimentary interfaces and have long been designed with a focus on safety over security. The controllers are not exclusive to construction and are commonplace in mining, transportation, material handling and manufacturing. Consequently, these sectors are equally susceptible to cyber threats. Transitioning towards wireless, standardised technologies emerges as a prudent step forward.

Jon Clay, vice president of Trend Micro emphasises the need for cybersecurity within the field: "The construction industry is becoming more and more run by technology and software. As such, companies need to ensure they are putting cyber security on their radar to ensure equipment such as cranes are protected from attack."

"Our research laid out a number of attack scenarios we thought could be used to target these cranes and even had some 'proof of concept' attacks that were successful. Hopefully the industry, dealers and manufacturers will take these into account and implement the suggestions we gave to secure them from attack."

Trend Micro's research outlined five distinct forms of attack, which may evolve as technology advances:

1. **Replay attack:** The attacker records RF packets and subsequently replays them to seize control of machinery.
2. **Command injection:** An attacker can modify the RF protocols to have complete control of the machines.
3. **E-stop abuse:** The attacker can replay emergency stop commands and in turn causing a denial-of-service (DoS) condition.
4. **Malicious re-pairing:** An attacker can clone a remote controller or its function to hijack a legitimate one.
5. **Malicious reprogramming:** The attacker 'trojanises' the software operating on the remote controllers to obtain full control.

A poignant reminder is an incident in 2021 involving Colonial Pipeline in the US, which paid a ransom of almost $4.4 million to Russian cybercriminals following a crippling cyberattack on its IT network. The disruption halted fuel deliveries along the East coast spanning 5,500

Trend Micro's research outlined five distinct forms of attack

miles of pipeline and caused significant disruption to fuel station restocking and airline operations. Joseph Blount, chief executive of Colonial Pipeline admitted that the software was not protected by multifactor authentication. The incident's relevance lies in its highlighting of the consequences stemming from inadequate cybersecurity protocols.

Colonial Pipeline in the US paid a ransom of $4.4 million to Russian cybercriminals following a crippling cyberattack on its IT network

In response to these looming threats, Trend Micro has released a comprehensive security checklist to guide users in safeguarding their systems. Key recommendations include thorough scrutiny of manuals before purchasing controllers to ensure configurable pairing options, immediate modification of pairing (ID) codes upon purchase, and a preference for devices that employ open, established standard protocols such as Bluetooth or 5G - providing inherent security.

NAÏVE PAIRING

All radio remote controllers are shipped with a pre-configured pairing code in the exchange packets to avoid protocol-level interferences while working on the same frequencies. This feature, however, does not offer any security measures. Trend Micro's research found that manufacturers could mislead customers when it comes to security features. One manufacturer for instance mentions that the pairing mechanism 'prevents messages from other radio equipment from activating any system function'. The hacking above proved otherwise.

Some RF controllers have a slightly more advanced security feature involving a passcode or a hardware key, however the Trend Micro team found that the start sequence is not protected by the password or hardware key, so an attacker could power on the machinery without the passcode. The proper way to secure RF controllers is to make sure all transmissions are authenticated and encrypted.

One of the manufacturer's in the report - HBC-radiomatic - does implement an authentication authorisation function which requires a smart card to gain access, although it could be said that even these can be lost, stolen or cloned.

HBC-radiomatic does implement an authentication authorisation function which requires a smart card to gain access

Finally, during field tests the team noticed that one tower crane had an infrared (IR) receiver mounted on its jib and aimed downwards at the ground. Some manufacturers use a 'virtual fencing' system using IR for secure communication, allowing commands only within the IR beam's range. Others use RF heartbeat packets to signal proximity between the remote control and crane. However, RF lacks the security of IR. In tests with Juuko controllers, the team replicated the heartbeat packets to trick the crane's receiver.

INDUSTRY ISSUES

According to the report, one of the main issues the industry will face is that because industrial radio devices have higher replacement costs and longer life spans than those aimed at consumers, these vulnerability issues are likely to persist for years and it is unlikely that the issues identified are rectified quickly, if at all. However, patching the devices is always possible.

Some of the manufacturers Trend Micro contacted have since improved the security of their equipment but it says there is a reluctance to fix issues due to high downtime costs and 'business continuity constraints'.

The possible long term solution is to move away from proprietary RF protocols and focus on standards such as Bluetooth Low Energy which is one of the main standard options. The benefit is the increased security level and subsequently less burden on the manufacturers to design or integrate custom RF protocols.

Users concerned about security risks should opt for a device that has virtual fencing features which disable the equipment when the remote is out of range. This would make hacking the equipment more difficult as the attacker would need to be on site or know when the transmitter is enabled to carry out the attacks.

Whatever your view, there is a genuine threat that looms over the crane or equipment sector. Let's hope it doesn't take a major incident to make people take the issue more seriously. ■