MITIGATION PLAN

Distribution Substation

Prepared by:

Darren T. Nielsen, CPP, PSP, PCI

August 8, 2019

NAVIGANT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On Tuesday, July 23, 2019, in response to the California Public Utilities Commission Order D-19-01-08, on Physical Security, Darren T. Nielsen, CPP, PSP, PCI, of Navigant Consulting, Inc., conducted interviews and a vulnerability assessment in reference to the Substation.

The purpose of the threat and vulnerability assessment is to identify electric distribution assets that may merit special protection, and measures to address potential security risks and reduce the potential of long-term outage to an identified distribution facility that meets the following criteria: *Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants).* BVES has no other substations that meet the other six CPUC criteria listed in the order.

These interviews provided additional insights for the assessor to process the information obtained from the Subject Matter Experts (SMEs) and helped to focus the site tour on ways a physical attack on the substation from outside the fence-line could occur, identify the vulnerabilities and critical assets of the Substation, and identify potential hostile surveillance points in the surrounding area.

The assessment included the 3 critical distribution assets of the facility and a 34kV feed line to uncover security weaknesses, and potential threats which could impact the BVES distribution capabilities should a physical attack take place. The following personnel listed below were consulted as the SMEs and interviewed as part of the assessment.

The Bear Valley Electric Service team consisted of:

Paul Marconi -Director

Jeff Barber -Field Operation Supervisor

The assessment is the source for the development of this Physical Security Mitigation Plan which identifies mitigation, protection, prevention and resiliency efforts to mitigate the risk of long-term outage to the Substation.

BVES has a very robust spare parts program that would significantly decrease any long term outage due to damage or physical attack. Additionally, BVES has a redundant path and ability to redirect load for increased resiliency to mitigate any short term outage.

NAVIGANT

MITIGATION PLAN

Purpose

This Mitigation Plan has been developed to address physical threats and vulnerabilities for the Substation which were identified in the Threat Vulnerability Assessment conducted on July 23, 2019.

Scope

The scope of this Mitigation Plan for the Substation is to:

- Identify and implement security measures to deter, detect, delay, assess, communicate, respond, and recover to potential physical threats
- Establish an incremental timeline for executing physical security enhancements and modifications to mitigate identified threats and vulnerabilities

THREATS AND VULNERABILITIES

Potential threats and vulnerabilities to physical attack have been evaluated for the Substation.

The threats and vulnerabilities were identified through a comprehensive assessment performed by Darren T. Nielsen, CPP, PSP, PCI, of Navigant Consulting, Inc.
.

The scope of the threat and vulnerability evaluation included:

- Identification of the site's critical assets
- Existing physical security measures
- Site and Asset vulnerabilities
- Unique site characteristics
- Prior history of attack on similar facilities
- Intelligence or threat warnings from law enforcement, NERC and E-ISAC
- FBI Uniform Crime Statistics

Based on an analysis of possibility, probability and impact of potential threat scenarios, the following threats and attack types of arson, ballistic fire, man-portable IED, sabotage and vehicle ramming were

considered in evaluating substation vulnerabilities along with the appropriate countermeasures and recommendations.

SECURITY SOLUTIONS

Deterrence

Deterrence is the act of discouraging individuals from attempting to gain unauthorized access to the facility by implementing measures that would be perceived as too difficult or needing special tools and training to defeat.

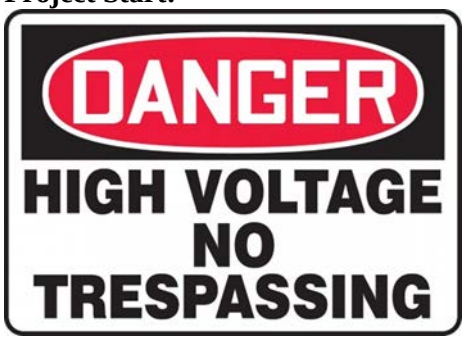
1. **Vulnerability**: "No Trespassing" warning signs are not installed on or beyond the fenced perimeter of the Substation. This creates a vulnerability by not informing encroachers that they are trespassing on BVES private property well before they reach the fenced perimeter.

   Mitigation: Install no trespassing signage on all perimeter sides

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Implementation: BVES will procure the new signs and install.

   Project Start: **Estimated Completion**:



2. **Vulnerability**: Overgrown vegetation provides concealment opportunities for would be adversaries. Removing vegetation would create a clear zone that will enhance natural detection, increase deterrence value as well as aid in CCTV assessment.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Remove and cut back vegetation 75 yards around the eastern and southern perimeters. Create a 10-yard clear zone around site's fenced perimeter

   Implementation: BVES will remove and control perimeter vegetation at the Substation.

   Project Start: **Estimated Completion**:

3. **Vulnerability**: Insufficient or inappropriate lighting presents a safety issue as well as a vulnerability for deterring and detecting malicious activity. Future CCTV enhancements may be hindered for assessing potential breaches and critical assets from the perimeter and beyond.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install security lighting onsite and integrate into the access control system, allowing for remote operation of the lighting for enhanced deterrence, detection and assessment capabilities. Ensure adequate lighting levels are achieved to support desired CCTV resolution.

   Implementation: BVES will work with staff security technicians to install additional lighting at the facility.

   Project Start: **Estimated Completion**:

Detection

Detection refers to the capability of identifying unauthorized access as early as possible by implementing measures to actively alert appropriate personnel if an unauthorized action is occurring or has occurred, and to facilitate a timely response.

1. **Vulnerability**: No ability to detect adversaries at the Substation perimeter or beyond outside of random surveillance tours or treatment facility staff observation when entering or exiting site.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

Mitigation: Install perimeter intrusion detection system at the BVES Substation to provide 24/7 encroachment and intrusion detection capabilities at the perimeter. Integrate the intrusion platform into the existing BVES video surveillance system, providing for automated event based intrusion detection and assessment capabilities.

Implementation: BVES will procure. video management system with analytics

Project Start: **Estimated Completion**:

2. **Vulnerability**: No ability to determine if movement outside perimeter is humanoid or animal

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install cameras and integrate into video management system with analytics for automatic alerting and assessment capabilities.

   Implementation: BVES will work internally with Technical support staff to project plan with installation.

   Project Start: **Estimated Completion**:

THERMAL CAMERA

3. **Vulnerability**: The manual gates are unmonitored with no reporting technology for when they are opened or to distinguish between authorized or unauthorized access.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Installation of gate contacts on all manual vehicle and man gates to be informed and/or alerted when gates have been opened.

Implementation: BVES will coordinate installation with Tech-shop and/or outside contractor

Project Start: **Estimated Completion**:

PHOTO REMOVED

Delay

Delay is distinguishable from a deterrent in that true delay can be measured after detection has occurred. Delay prior to detection is a deterrent. Effective delay countermeasures slow progress of an attack as long as necessary to allow a security response to be activated by implementing security measures to slow the progress of harmful events.

1. **Vulnerability**: Perimeter fence is standard chain link which provides minimal delay (7-10 seconds) and visual obscurity of critical assets.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install or retrofit to an anti-climb/cut, 12' high, tight mesh to obscure sites assets, increase delay value and act as a deterrent.

   Implementation: BVES will work with current vendors to assess.

   Project Start: **Estimated Completion**:

2. **Vulnerability**: Vehicle gate can be easily breached by either personal vehicle or heavy construction equipment.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Implement a crash rated vehicle gate or ensure facility maintains the access gate in a closed or controlled position

   Implementation: This will be a stakeholder engagement meeting to discuss options.

   Project Start: **Estimated Completion**:

3. **Vulnerability**: Commercial Grade Padlocks can be easily compromised by unpowered hand tools.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device

Mitigation: Replace current long shanked padlocks on all man-gates with a shroud protected shank padlock that prevents the use of bolt cutters.

Implementation: BVES will replace all padlocks with a higher security shroud padlock on all perimeter access points.

Project Start: **Estimated Completion**:

4. **Vulnerability**: High Speed Approach by vehicle can breach fence-line and enter site.

   Associated Threats: sabotage, explosive device, vehicle attack

   Mitigation: Install concrete jersey barriers or decorative boulders to create crash resistant barriers at the most likely avenues of approach outside the fence-line along the East and southern borders

   Implementation: Schedule work with BVES Maintenance to install on the fence-line.

   Project Start: **Estimated Completion**:

5. **Vulnerability**: Metal Key Control is inadequate with numerous unaccounted for keys (1AB).

   Associated Threats: sabotage

   Mitigation: Transition to electronic smart keys in lieu of hard keys and implement a key management system. Smart keys will give the option to track and report on access to critical areas as well as be able to remotely disable if lost or stolen.

   Implementation: BVES will use a phase approach and cover upfront initial launch.

   Project Start: **Estimated Completion**:

6. **Vulnerability**: Critical Assets are easily identified and visible through view fencing which provides line of Sight (LOS) to an attacker.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Transition the critical assets to inside a pad mounted locked cabinet such like they were at nearby BVES substation.

   Implementation: BVES will install pad mounted assets during the substation upgraded process

   Project Start: **Estimated Completion**:

Assessment

Assessment is the act of identifying whether a detected individual or onsite activity is authorized, or if a response by contract security or law enforcement is necessary.

1. **Vulnerability**: No camera coverage of the critical assets and fence-lines.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install cameras to increase site coverage

   Implementation: BVES will plan the most efficient use of fixed or PTZ cameras, and/or fixed FLIR day/night thermal IR cameras to ensure appropriate coverage of the site and critical assets.

   Project Start: **Estimated Completion**:

Communicate

Communicate is the act of informing a detected individual that is in an unauthorized area, that their presence is known and that they need to depart immediately. It also refers to the process of alerting internal and external resources, including law enforcement of a potential security breach.

1. **Vulnerability**: No audible alarm notification or talk-down PA capability at the site.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install PA intercoms onsite to ensure a communication response.

   Implementation: BVES will install one device to effectively communicate and enhance a response

   Project Start: **Estimated Completion**:

2. **Vulnerability**: No visual alarm notification at the site to indicate that the intruder has been detected.

   Associated Threats: Arson, ballistic attack, sabotage, explosive device, vehicle attack

   Mitigation: Install a Strobe/Sirens on the site and integrate into video system.

Implementation: BVES will select product technology and schedule work with technology staff for installation.

Projected Cost: $5K - $7k **Estimated Timeline**: Q2 2020

Response

An effective response counters the anticipated activity of an unauthorized person within a time appropriate by implementing measures to prevent, resist, or mitigate the impact of an attack or event.

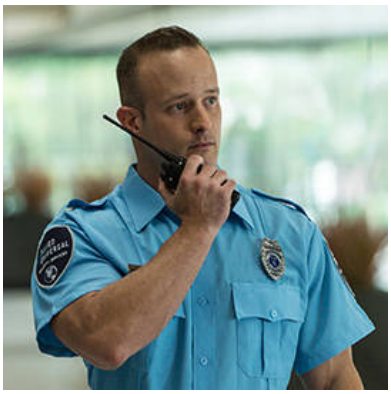
1. **Vulnerability**: The site does not have 24/7 onsite security officers or a documented coordination plan with law enforcement. Each of these items increases response time, decreases the likelihood of an efficient and effective response.

   Associated Threats: Arson, Ballistic attack, explosive device, sabotage, vehicle attack

   Mitigation: Add roving security patrols and/or augment onsite periodic visit coverage.

   Implementation: BVES will work with Staff to ensure additional visibility at the site.

   Project Start: **Estimated Completion**:



SECURITY REFERENCES

- California PUC Senate Bill No. 699
- ASIS Protection of Assets
- ASIS Physical Asset Protection ANSI/ASIS PAP.1-2012
- Dept. of State SD-STD-02.01 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates
- ASTM F-2656-07 Vehicle Crash Testing of Perimeter Barriers

PRE VS. POST MITIGATION

A means to evaluate the effectiveness of the proposed security improvements is to quantify the risk reduction of security mitigations. The methodology used for this assessment references risk methodologies developed by federal agencies, which define the Likelihood of Successful Attack (LSA) as the combination of Threat, which is the likelihood of an attack or event occurring, and the Vulnerability, which is the likelihood of the attack or event being successful. Risk reduction is achieved by decreasing the LSA. Risk reduction ratings in the following table compare the LSA before and after implementation of all mitigations.

Attack Type	Attack Likelihood (AL)	Facility Attractiveness (FA)	Threat (AL x FA)	Vulnerability	LSA (Threat x Vulnerability)
Arson					
Pre-Mitigation	2	6	12	8	96
Post-Mitigation	2	3	6	3	18
Ballistic Attack					

Pre-Mitigation	3	9	27	9	243
Post-Mitigation	3	2	6	6	36
Explosive Device					
Pre-Mitigation	1	6	6	8	48
Post-Mitigation	1	3	3	3	9
Sabotage					
Pre-Mitigation	4	8	32	9	288
Post-Mitigation	2	2	4	6	24
Vehicle Attack					
Pre-Mitigation	2	6	12	5	60
Post-Mitigation	2	2	4	3	12

Attack Likelihood Criteria

Very High (10)
• **Intelligence** - Credible intelligence has indicated developing plotting. • **Presence** - Group has a large presence in the Western region. • **Intent** - Group has made recent public statements or showed signs of intent that may negatively impact the company. • **History** - Group has recently conducted, planned, or facilitated recent criminal activities against the company. • **Capability** - Group possesses a high capability or material resources to negatively impact the company involving the threat vector.
Medium (5)
• **Intelligence** – Intelligence may be interpreted in various ways, has alternative views, or the information is credible and plausible, but not corroborated sufficiently to warrant a higher level of confidence. • **Presence** - Group has a moderate presence in the Pacific Northwest region or within the Western U.S. • **Intent** - Group has made past public statements or showed signs of intent that may negatively impact the company. • **History** - Group has previously conducted, planned, or facilitated criminal activities against the company. • **Capability** - Group possesses a moderate capability or material resources to negatively impact the company involving the threat vector.
Very Low (1)

- **Intelligence** – The information is scant, questionable, or very fragmented and it is difficult to make solid analytical inferences, or there are significant concerns or problems with the sources.
- **Presence** - Group has an insignificant presence in the Pacific Northwest region.
- **Intent** - Group has made not made recent public statements of intent that may negatively impact SCG or the natural gas sector in general.
- **History** - Group has conducted, planned, or facilitated minimal or no criminal against the company or the energy sector.
- **Capability** - Group possesses a low capability or material resources to negatively impact the company or the energy sector.

Facility Attractiveness Criteria

Very High (10)
• **Perception of security** - the adversary may determine a **very high** likelihood of success derived from the perception of ***minimal*** layers of ***basic*** security features. • **Perception of value** - there is a ***very high*** likelihood of identifying high value commodities (i.e., copper, tools, and man portable equipment) and/or infrastructure which appears to be of operational importance (i.e., transformers, above ground pipelines, control shelters).
Medium (5)
• **Perception of security** - the adversary may determine a ***moderate*** likelihood of success derived from the perception or observation of ***some*** layers of overt security features. • **Perception of value** - there is a ***moderate*** likelihood of identifying high value commodities (i.e., copper, tools, and man portable equipment) and/or infrastructure which appears to be of operational importance (i.e., transformers, above ground pipelines, control shelters).
Very Low (1)
• **Perception of security** - the adversary may determine a ***very low*** likelihood of success derived from the ***observation*** of ***multiple*** layers of overt security features that are present and appear to be functional and in good repair. • **Perception of value** - there ***very low*** likelihood of identifying high value commodities (i.e., copper, tools, and man portable equipment) and/or infrastructure which appears to be of operational importance (i.e., transformers, above ground pipelines, control shelters).

Vulnerability Criteria

Very High (10)
Existing physical security countermeasures ***would not prevent*** the threat from accomplishing its primary objective(s), providing a ***very high likelihood of success***. The facility has ***minimal access, detection, and***

interdiction capabilities. Guidelines for poor physical security countermeasures may include, but not limited to, the following:

- ***Access*** - There is free public/vehicle access and no restrictions on articles that may be carried. There is no perimeter control, and the asset is void of physical barriers. There are no guards or patrols available to deny access.
- ***Detection*** – No authorized guards, employees, or public presence (to observe suspicious activity/items). The asset is not equipped with CCTV or intrusion systems. The asset and surrounding area are insufficiently illuminated.
- ***Interdiction*** – There is no emergency response planning. Response personnel or equipment are not available. Timing available to interdict the attack is insufficient [e.g., suicide attack].

Very Low (1)

Existing physical security countermeasures ***would prevent*** the threat from accomplishing its primary objective(s), providing a ***very low likelihood of success***. The facility has ***significant access, detection, and interdiction capabilities***. Guidelines for excellent physical security countermeasures may include, but not limited to, the following:

- ***Access*** - The asset has an established perimeter with impenetrable physical barriers and guards at all entry points. There is card reader access with ID verification, and all cleared personnel have had a thorough background investigation.
- ***Detection*** – Significant authorized personnel or public presence (to observe suspicious activity/items). All personnel and the public are aware of restricted areas due to marked signs/postings, training, or otherwise. All entering vehicles, personnel and baggage are screened. The asset is equipped with CCTV with onsite 24/7 monitoring, and intrusion systems. The asset and surrounding area is sufficiently illuminated.
- ***Interdiction*** – The threat is reported to response forces immediately upon detection. The time line allows for interception of the attack. Communication equipment for personnel and the public is readily available to report suspicious activity. Response plans cover multiple situations and personnel are readily available, trained, and equipped. Response personnel receive refresher training, conduct exercises, and have back-up equipment.

DATA SHEETS

The following Data Sheets will provide more information on the various mitigation options discussed above.

Chameleon Fence

Amiguard Fence System™ Patent Pending
Steel Security Fencing

Alabama Metal Industries Corporation ® October 1, 2016

PART 1 GENERAL

1.01 SCOPE OF WORK
Supply and install all materials and accoutrements required for the new construction of an aesthetic and seamless high security fence system.

1.02 SYSTEM DESCRIPTION
The Amiguard System® shall be installed providing the height of barrier as noted on drawings. The supply of mesh fabric, framework and accoutrements for the attachment of mesh to framework, and their respective coating shall be supplied by one source to ensure the quality and level of security required. The fence system shall incorporate high strength Infini-Rails™ that pass through vertical posts without any mesh-to-mesh overlaps between posts. The high security fence shall consist of a mesh fence fabric of a specified height made from sheet steel that is simultaneously slit and stretched into a rigid, open mesh diamond making one continuous sheet. The finished shape of the mesh openings shall be diamond. Conventional expanded metal not manufactured specifically for security purposes is NOT permitted for this use.

1.03 REFERENCES
All components shall meet or exceed the following standards: ASTM F1267 (Tolerances for Mesh Panels) Type 1, Class 2.
ASTM A 123 (Zinc Coating) Standard Specification for Zinc Coatings on Iron and Steel Products.
ASTM A500 (Framework) Standard Specification for Cold-Formed Welded and Seamless Carbon Steel Structural Tubing in Rounds and Shapes.
ASTM A 1011 (Accoutrements) Specification for Steel, Sheet and Strip, Hot-Rolled, Carbon, Structural High Strength Low Alloy with Improved Formability.

1.04 SUBMITTAL
Submittals shall include brochures, details, specifications, test reports and samples as required prior to ordering.

1.05 QUALITY ASSURANCE
Dealer / Installer shall provide project management and laborers experienced, certified and approved in the installation of AMICO Amiguard Security Fencing System® as specified.

1.06 STORAGE AND HANDLING
Materials shall be stored in a clean dry location with proper ventilation to avoid damage from moisture. Materials shall be protected against damage from weather, vandalism, and theft. Any freight damage must be noted immediately on bill of lading.

PART 2 MATERIALS

2.01 MANUFACTURER
ALABAMA METAL INDUSTRIES CORPORATION, (AMICO),
3245 Fayette Avenue - Birmingham, AL 35208
Telephone 855-552-6426 - Facsimile 205-783-9507
www.amicosecurity.com

2.02 MESH DESCRIPTION
1. Minimum mesh dimension - 0.180 inches
2. Maximum mesh dimension – 0.800 inches
3. Maximum mesh opening - 25% open area
4. Maximum mesh screening - 75% closed area
5. Galvanized weight - as specified by manufacturer

AMIGUARD FENCE SYSTEM™

7100 Series

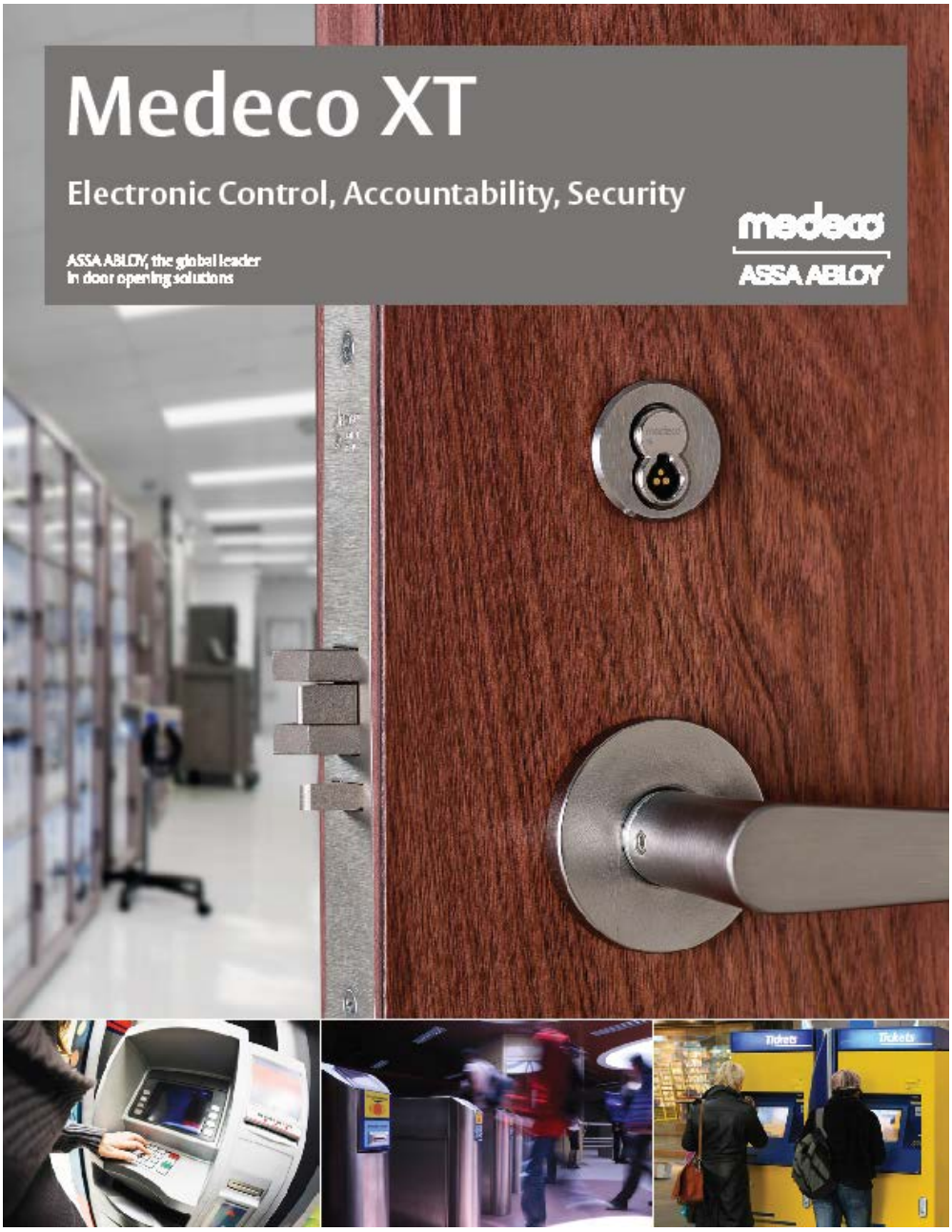
2.03- FRAMEWORK
1. Slotted posts and Infini-Rails shall be 58,000 PSI structural tubing per ASTM A500. AMICO Secura-Sleeves allow rails to slide through posts for fast easy installation.
2. Mesh panels secure to rails using Diamond Fasteners and carriage bolts.
3. Finish Plates field fit to posts allowing mesh attachment creating a unitized perimeter security barrier.

2.04 FINISH
1. Hot dip galvanized to ASTM A123.
2. Color Coated 8-11 heavy mil black finish as produced by AMICO using the 4-Step Trinity Plus application process.

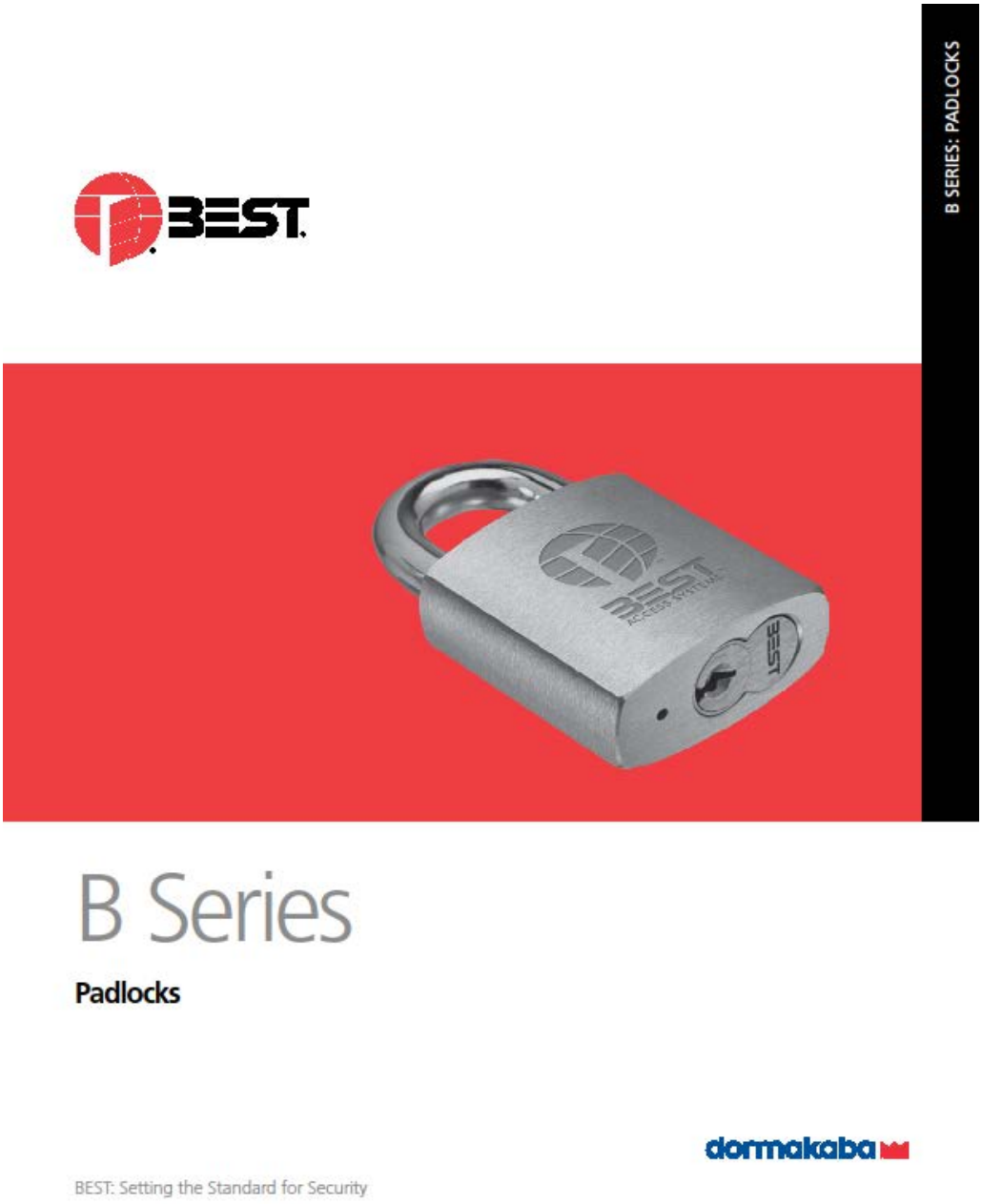
PART 3 INSTALLATION
Secura-Sleeves snap on to Amiguard posts and allow AMICO Infini-Rails to pass through the post easily. Sleeves prevent water from entering the post. Rails are bolted together making a continuous rail for the length of the fence run. Mesh panels fit in between posts and are bolt to rails using Diamond Fasteners and carriage bolts. Finish Plates are secured to posts with tamper resistant self-drilling screws. Carriage bolts are used to secure mesh panels to plates completing the installation of framework and mesh panels. Seat flat top post caps on each post. Install gates as required.

FLIR Camera

Medeco XT Keys



BEST Padlocks



AXIS PTZ Cameras

Datasheet

AXIS COMMUNICATIONS

AXIS Q6215-LE

Heavy-duty PTZ camera with OptimizedIR

AXIS Q6215-LE PTZ Network Camera has a ½-inch sensor and combines great image quality with fast panning, tilting, and zooming. Its powerful, built-in IR illumination allows for an impressive viewing range in total darkness (up to 400 m or 1300 ft). This camera is ideal for open-area surveillance, since its robust design can withstand the toughest weather conditions including wind speed up to 245 km/h (150 mph). AXIS Q6215-LE is compliant with IP66, IP68, IK10, and NEMA 4X. It can be mounted facing up or down and comes equipped with a wiper to remove excess water, rain, or snow.

> HDTV 1080p with 30x zoom
> Long-range OptimizedIR
> MIL-STD-810G compliant
> AXIS Guard Suite analytics
> Zipstream, Lightfinder, and WDR

ONVIF | HDTV NETWORK VIDEO

AXIS IP Public Address Speaker

Datasheet

AXIS C3003-E Network Horn Speaker

Clear and simple

AXIS C3003-E Network Horn Speaker is a simple-to-install outdoor loudspeaker that provides clear, long-range speech for remote speaking in live video surveillance. Audio can be manually or automatically triggered in response to an alarm, and deter unwanted activity through pre-installed or uploaded audio files. The loudspeaker has an integrated amplifier and combines low power consumption with high sound pressure. AXIS C3003-E integrates easily with SIP (Session Initiation Protocol) Voice over IP (VoIP) systems and video management software (VMS) supporting audio. Several speakers can be connected in a zone with synchronized audio using only one IP address for the leader speaker.

> Simple installation with PoE

> Easy VMS integration

> Supports open standards – VAPIX, ACAP, SIP

> Reliable Auto Speaker Test