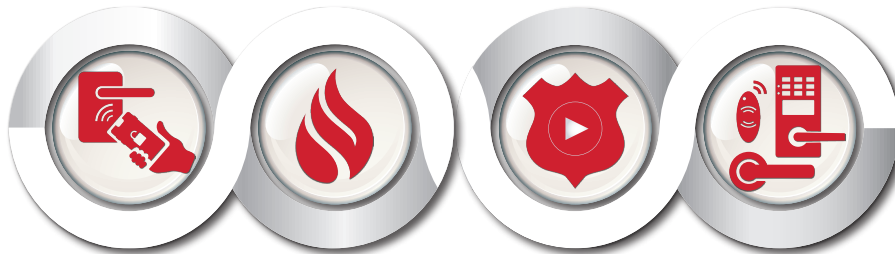

WHITE PAPER



**Access
Control**

**Commercial
Fire**

**Intrusion
& Video**

**Locking &
Hardware**

Comprehensive Methods for Integration to Napco Security Technologies Solutions



Introduction

Napco Security Technologies, Inc. (NASDAQ: NSSC) is a publicly-traded company, consisting of four divisions and its own vertically-integrated 200,000 square foot, ISO:9001 certified manufacturing facility, purely dedicated to the security industry. The major products of Napco Security include Intrusion and Fire Control Panels, Cellular based Communication devices, Stand-alone and Wireless Networked Locking products, Cloud Based Security Software and Service products, Access Control Panels and Software and Video Products and Services. Napco Security designs and develops its own products and maintains fully owned manufacturing facilities, with corporate headquarters located in Amityville, NY.

This white paper will discuss the various methods for integrating to the divisional products of Napco Security Technologies, Inc. These methods include Software API Integration, Import/Export Utilities, and SDKs for Direct Integration to Napco controller and locking hardware products.

The SDK method of direct integration to Napco Security hardware products provides the opportunity of entering into an OEM hardware relationship with Napco Security, called the Black Box Program (see the Black Box Program sections noted below).

It should be noted that there are also many product specific, dedicated coded Integrations from some Napco Security products to other Napco Security products and also other security brand products and related industry products. For more information on these integrations, see the Napco Security divisional websites (website links shown below).

Napco Security Technologies divisions, major brands and product lines:

Napco Security Systems (www.napcosecurity.com):

- GEM Intrusion Panels
- GEMC (Commercial) Intrusion and Fire Panels
- Prima Intrusion Panels
- iBridge Apps and Video Products
- Connected Home (Napco and Prima)
- StarLink Cellular Communicators (Universal, Intrusion and Fire)
- Napco Cloud NOC for StarLink Communicator
- NA-E Linux Embedded Access Controllers (1DM, 2DM, 4DM and 8DM)

Alarm Lock (www.alarmlock.com):

- Trilogy Electronic Door Locks
- Trilogy Networkx Wireless Locks
- ArchiTech Networkx Wireless Locks (Marks USA Lock Bodies) and Wireless Netpanel
- DL-Windows Software (supports Trilogy & Architect Locks) and iLock App
- Air Access Cloud Software and App

Napco Access Pro (formerly Continental Access)(www.napcoaccesspro.com):

- Controllers: CA-1, CA-2, CA-4, and CA-8/CA-16
Continental Access Enterprise Control Panels
- CA4K Enterprise Access Control Software for Continental Access Control Panels and Alarm Lock Networkx and ArchiTech Wireless Locks and Wireless Netpanel
- CA4K App and iLock for Continental App
- MVP Enterprise Cloud Access Control Software for Continental Access Enterprise Panels and Networkx & ArchiTech Wireless Locking.
- CA-E Linux Embedded Access Controllers (1DM, 2DM, 4DM and 8DM)

Marks USA (www.marksusa.com):

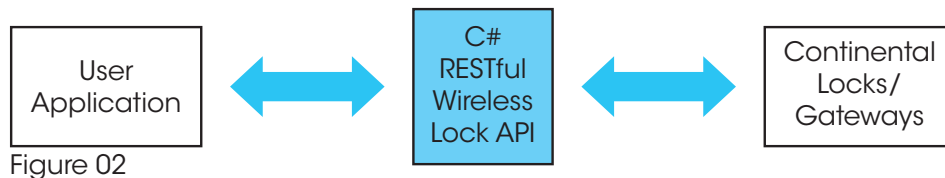
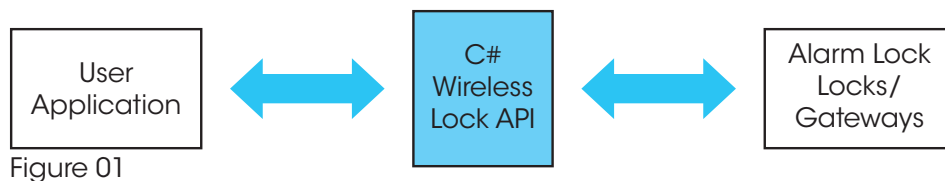
- LocDown Series Locks
- Survivor Series Cylindrical Locks
- LifeSaver Series Cylindrical, Mortise and Anti-Ligature Locks
- ArchiTech Networkx Wireless Locks (Alarm Lock Wireless Electronics) – complete Grade-1 Architectural Wireless Locking.
- Design-a-Lock Custom Locksets and Accessories

Integration to Napco Security Division Products

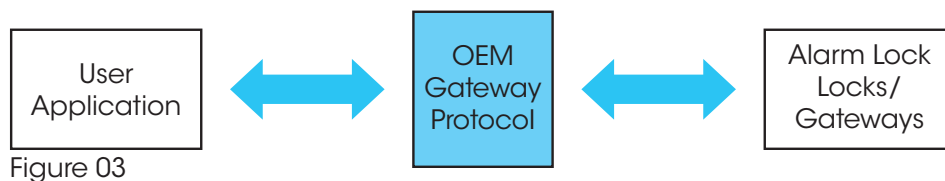
Integration to Napco Security Systems products is focused towards the Napco GEM and GEMC product lines, where a Napco GEM API can be used to send commands to a Napco GEM Z-Remote/I-Remote or Netlink device, connected to the GEM hardware and automation software environment.

Integration to Alarm Lock and Marks USA Division Products

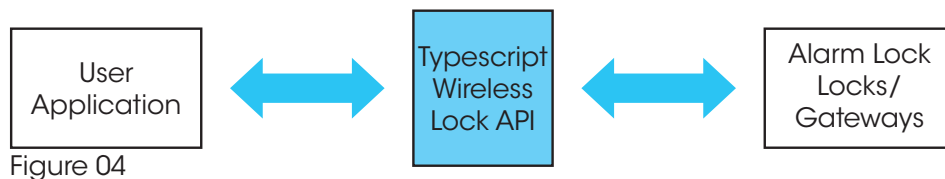
Integration to Alarm Lock products is focused towards the hardware of the Networkx and ArchiTech Wireless Lock product lines. Integration to Alarm Lock Networkx and ArchiTech hardware can be most quickly accomplished through the Continental Access CA4K platform, see the Integration to Napco Access Pro section, for both the C# Windows API and the C# Windows RESTful (IIS) API options. These integrations rely on the Continental Access CA4K software and SQL environment for the basic configuration and maintenance of the locking hardware. For integration to Alarm Lock Networkx and ArchiTech hardware in a nonContinental environment, there is a Windows C# API and Windows C# RESTful (IIS) API, that require moderate development. Both of these APIs have an installer. The C# API allows for development in a Windows environments only and the RESTful API allows for development on any platform. See Figures 01 and 02 below.



If it is desired to have direct, low-level integration to the Alarm Lock Networkx and ArchiTech hardware, there is an OEM Protocol available, accompanied by full documentation. This approach allows for more seamless integration to the locking products, but requires the most development to fully discover and configure the hardware and to completely maintain the Personnel and Credential environment at both the server and target hardware.



Additionally, there is a Typescript RESTful Lock API. The Typescript RESTful API has an installer program and operates on a Node.js server and a Postman software example is provided.

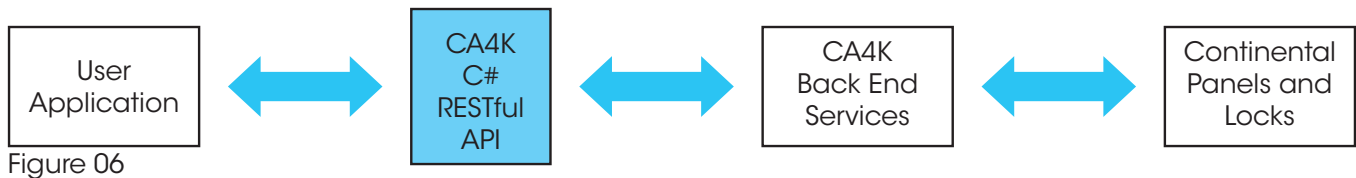
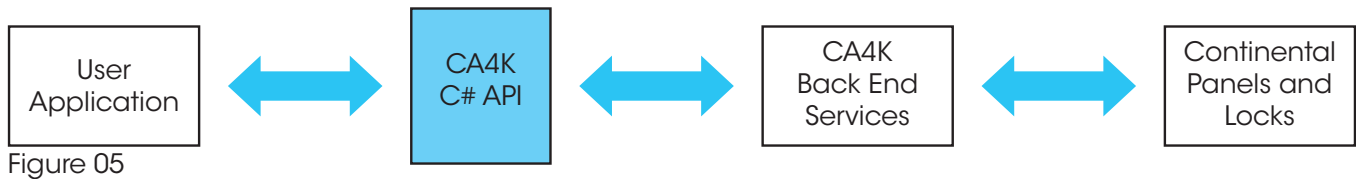


For developing the integration to Alarm Lock Networkx and ArchiTech hardware by any of the methods above, an SDK is available, comprised of the appropriate documentation, a Networkx Wireless Gateway, a Networkx Wireless Expander, a Networkx Wireless Lock and an ArchiTech Wireless Lock is available (P/N: SDK-AL-xxxx).

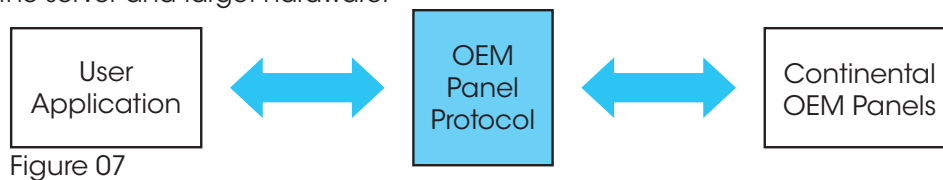
All of these integration methods allow for real-time control of the locking environment, adding user credentials, setting time schedules for automated control of doors, and issuing on-demand manual commands for controlling doors, including issuing lockdowns of the system.

Integration to Napco Access Pro (formerly Continental Access) Division Products

Integration to the Napco Access Pro controllers and the Alarm Lock Networkx and ArchiTech Wireless Locking hardware in the Continental environment can be accomplished with either a C# API for Windows or a C# RESTful (IIS) API. The CA4K environment is based on an SQL Database schema. Both of these APIs also have an installer. The C# API allows for development in a Windows environments only and the RESTful API allows for development on any platform. See Figures 05 and 06 below. These integration methods allows for real-time control of both the hardwired Access Control Panels and Alarm Lock locking environment, adding user credentials, setting time schedules for automated control of doors, and issuing on-demand manual commands for controlling doors, including issuing lockdowns of the system.



If it is desired to have direct, low-level integration to the Continental Access Panels and Alarm Lock Networkx and ArchiTech hardware in a Continental Access environment, there is an OEM Protocol available, accompanied by full documentation. This approach allows for more seamless integration to the locking products, but requires the most development to fully discover and configure the hardware and to completely maintain the Personnel and Credential environment at both the server and target hardware.



For developing the integration to the Continental Access CA4K hardware by the methods above, an SDK is available, comprised of the appropriate documentation, a CA-1 controller, a CA-2 Controller and a CA-8 Controller (P/N: SDK-CA-xxxx).

NAPCO Security Technologies, Inc. © NAPCO 9.2024. Preliminary info subject to change without prior notice. Alarm Lock Trilogy, Networkx, Networkx ArchiTech, Lifesaver, LocDown & MVP Access are trademarks of NAPCO. All rights protected. Not for reproduction.

