WHITE PAPER | 12.17.2020

# Secure, Touchless Access Control with Face Recognition

by Walter Candelu

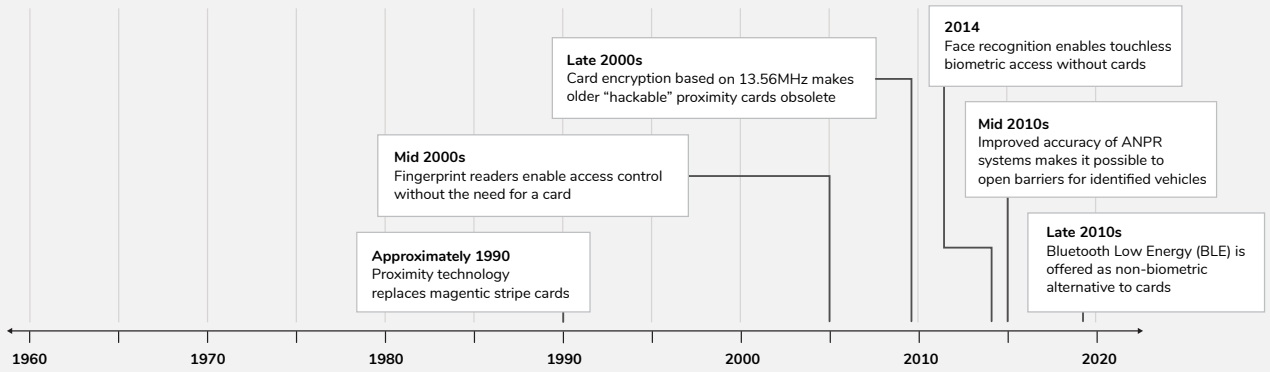
SAFR from realnetworks

# Contents

# Introduction

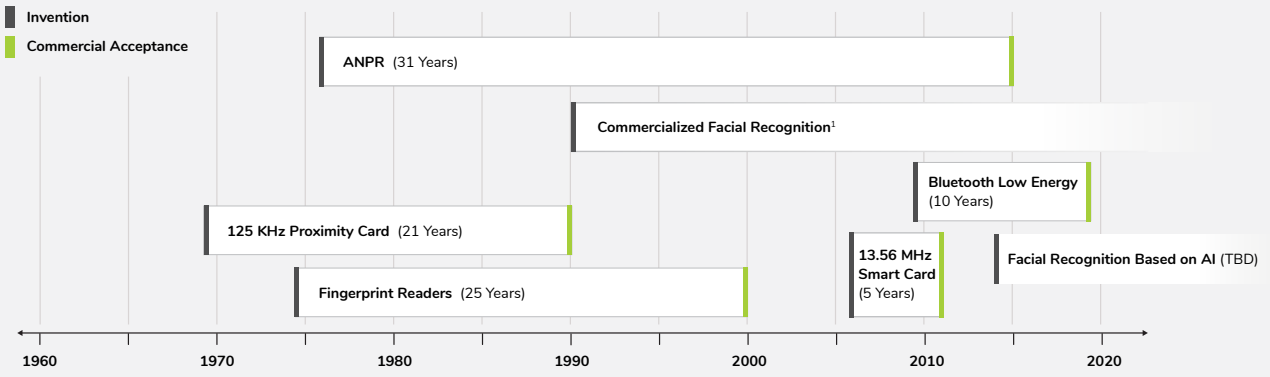
In recent years, disruptive technologies have equipped security professionals with innovative solutions to improve operational efficiency and increase the perception of security among users. The exponential progression of technologies in the access control sector illustrates this well:

**Progression of technologies in the access control sector**




Looking at this timeline with a different frame, it's easy to see that each technology took years from its invention to acceptance and eventual wide consumer use.

**Time from invention to wide use**




[1] Means by which to systematically measure and describe facial features for cataloging of identities was first practiced by Alphonse Bertillon in 1893 as part of his Portrait Parle anthropometric identification technique. It led the way to future semi-automatic and automatic approaches in 1964, Bledsoe et al., 1988 Principle Component Analysis (Kirby, Sirovich), 1991 Eigenface (Turk, Pentland) and others.

The time it takes for technologies to reach widespread use can be characterized by a period of declining technology costs leading to greater accessibility, coupled with growing consumer acceptance and familiarity. All technologies, in fact, must go through a sort of "5 stages of innovation denial" (denial, acknowledgement, acceptance, integration, enthusiasm) and in all cases, once the security professional and the end-user are aligned with the technical and operational benefits, the adoption process and market disruption become inevitable.

Face recognition is no different, and its unique benefits for customers in secure access use cases make its adoption inevitable as the next entry in the timeline of progression in the access control industry.

## Scope

This white paper will address all key operational and technical elements that make face recognition the ideal solution for security professionals looking to take their access control solution to the next level. It will also cover ethical considerations and privacy measures that will accelerate acceptance from end users.

**Operational**

- Touchless is better
- Ease of implementation and use

**Techno-commercial**

- High accuracy
- Ability to recognize masked faces
- Integration with legacy systems
- Robustness
- Liveness detection and anti-spoofing

**Ethical**

- Data privacy
- Ethical use & reducing bias

**Additional benefits**

- Repudiation and audit
- Support for multiple use cases
- Physical and logical access control
- In-person and remote authentication

## Touchless is Better

Since cards can be forgotten, lost, or misused, card credential technologies (Proximity/Mifare) have been replaced — or at least complemented — by biometric fingerprint credentials. Until 2019, fingerprint biometric credentials were widely accepted with limited risk and pushback.

However, amid a global pandemic that is redefining so many aspects of our daily lives, many businesses have disabled fingerprint readers to avoid possible spread of the virus. With a growing consumer desire for touchless experiences from point of sale, to hardware fixtures, to physical access

control, security companies are looking towards alternative technologies like Bluetooth credentials and face recognition to thwart both traditional security threats and virus transmission.

## Bluetooth Low Energy

There are multiple benefits to working with BLE readers and mobile credentials and this technology quickly became popular — especially among younger generations with higher rates of ownership and use of Bluetooth-enabled devices.

However, like many other technologies, BLE credentials come with its own challenges, for example:

- If your device battery is low or dead, it is rendered unusable.
- Just as with ID cards, phones are physical devices that can be forgotten, lost, stolen, or intentionally exchanged to allow access to unauthorized individuals[2].
- Any technology dependent on a physical item is not an entirely frictionless or touchless experience as it requires your device to be in hand, not in your pocket or backpack.
- Phones contain personal data — account numbers, photos, correspondence — prompting concern from some users over giving access to additional applications such as the authenticating technology used to confirm an identity.

While BLE technology is gaining momentum in the industry, it is still in the infancy stage and may find resistance from high-security implementations and consumers alike, without offering a truly deviceless, touchless secure access experience.

## Face Recognition

Like fingerprint biometric credentials, face recognition uses a unique biometric attribute — your face — which cannot be lost or shared and is always readily available. Moreover, face recognition has key advantages compared to fingerprint credentialling:

- It is touchless
- It is extremely fast and frictionless
- It is auditable and allows security staff to confirm the authentication event with a visual review if necessary

Touchless systems are invaluable during a global pandemic, but as the world is now more attuned to the dangers of high-touch surfaces and disease transmission points in public spaces, we can expect contactless technology to be preferred long after a vaccine for COVID-19 is developed. The world has been altered by the scope and scale of this pandemic and health and safety policies will have a stronger impact on building design and public behavior for years to come.

[2] Note, this can be solved by adding dual authentication with biometric credentials via the device.

### How Face-based Authentication Compares to Other Methods

| | Secure Access Method | | | |
|---|---|---|---|---|
| **Benefits** | **Badge/Key** | **Pinpad** | **Fingerprint** | **Face-based** |
| Authentication of an authorized individual and door control | ✓ Transferrable | ✓ Transferrable | ✓ | ✓ |
| Audit trail | ✓ Transferrable | ✓ Transferrable | ✓ No tailgating record | ✓ |
| Tailgating detection | ✗ | ✗ | ✗ | ✓ |
| Occupancy counting | ✗ Undercount if tailgating, no exit count | ✗ Undercount if tailgating, no exit count | ✗ No tailgating record | ✓ |
| Touchless | ✓ | ✗ | ✓ Certain solutions have been made touchless[3] | ✓ |
| Mask detection | ✗ | ✗ | ✗ | ✓ |

## Overcoming Misconceptions about Face Recognition

As outlined in the next sections, negative perceptions of face recognition do pose challenges. However, these can be overcome with the right facial recognition solution — and better education about how far this technology has come. Key misconceptions center around:

- Total cost of ownership
- Ease of implementation and use
- Data privacy
- Ethical use and reducing bias

### Total Cost of Ownership

One misconception is that a facial recognition solution with enterprise accuracy and speed is complex and expensive to purchase, deploy, and maintain.

[3] Touchless fingerprint readers have not been considered in this paper due to the comparatively high per-device cost of deployment which may limit broad adoption.

Despite the drastic reduction in required hardware resources driven by the introduction of artificial intelligence, it is true that face recognition is still a compute-demanding application. The three steps combined demand a large amount of computing power:

1. Live video processing
2. Face detection
3. Face recognition

To achieve enterprise-level performance, all three steps must be performed efficiently.

But not all facial recognition platforms are created equally. It is important to choose a system that is as efficient and compact as it is fast and accurate.

THE SAFR SOLUTION

## Total Cost of Ownership

SAFR's compact model and biometric template sizes, along with ultra-efficient processing, enable system integrators to deploy solutions that meet operational requirements using task-appropriate and cost-effective hardware. SAFR's biometric matching, watchlist management, alerting, and solution administration for real-time facial recognition use cases can be deployed on-premise, in the cloud, using NVIDIA Jetson, iOS and Android platforms, and emerging consumer and commercial devices built upon the Ambarella CV22 and CV25 chipsets.

**Video Processing Efficiency**

SAFR video processing benefits from RealNetworks' 25+ years of experience in streaming media. RealNetworks technology powered the first-ever live stream — a baseball game between the Seattle Mariners and New York Yankees in 1995 — before it became RealPlayer. This experience in video compression for streaming is directly relevant to the efficient video processing SAFR achieves today as the leader in face recognition for live video.

**Face Detection**

With SAFR 3.0, RealNetworks has launched a new high sensitivity face detector and improved recognition models specifically developed for matching faces when the lower half is covered by a virus transmission preventing face mask. SAFR's detection rate for faces in the wild that are partially covered by a mask now exceeds 95.1%. This includes surgical face masks as well as non-surgical fabric masks of varying patterns.

The new face detector also increases the efficiency of the algorithm such that dense scenes — with many faces visible in a single frame of video — are no more computationally intense than frames of video containing just one or two faces.

## Ease of Implementation and Use

The second face recognition misconception is the complexity of its implementation.

Many security professionals that came across facial recognition projects earlier in their career may have witnessed first-hand how early facial recognition systems were hard to install, configure, and operate. They often required dedicated cameras specifically deployed to capture an entirely front-view face image, could be difficult and expensive to integrate, and frequently failed to meet speed and accuracy expectations, preventing security teams from responding in real time.

But leading facial recognition systems have overcome these challenges, allowing security professionals to take advantage of the latest technology without needing to be experts in AI or having specific software programming skills.

THE SAFR SOLUTION

### Ease of Implementation and Use

SAFR can be installed on any major OS (Windows, Linux) as well as iOS and Android devices and can be deployed on a single computer to monitor a handful of IP cameras, or scaled to thousands of cameras to meet the challenges security professionals face when safeguarding large areas.

SAFR Actions make it easy to respond to recognition events with highly customizable actions and alarms in real-time such as: Unlocking a door for an authorized person, turning on lights when somebody enters a room, sounding an alarm when a known threat is detected, denial of entry for unregistered persons, triggering security SOPs, initiating a building lockdown, and more.

## Data Privacy

Personal Identifiable Information (PII) are unique identifiers — any information that can be used to identify, contact, or locate a specific person.

Examples of PII include, but are not limited to:

- Name and surname

- ID numbers: Passport number, driver's license number, credit card number
- Personal address information: Street address or email address
- Personal telephone numbers
- Social media account handles
- Biometric data: Fingerprints, iris scans, voice signatures, face images, or biometric signatures

In the digital age it is difficult to maintain complete anonymity and control over one's PII. Most people have public presences on LinkedIn, Twitter, Instagram, professional websites that contain photos, contact information, and additional PII that they have willingly uploaded for public or semi-public access. And virtually every online experience from purchasing an item online to managing banking and other sensitive transactions leaves a digital paper trail of PII vulnerable to hacking.

Like for fingerprint registrations, solutions using face recognition for access control must follow the strictest data security measures, acquire express consent from users, and ensure their data is used in accordance with the local legal frameworks. Operational requirements may include communication to users about the duration of data retention and opt-out options as well as control and access to their PII within the system. These policies should be thoughtfully developed and periodically reviewed.

THE SAFR SOLUTION

## Data Privacy

SAFR has been designed with privacy in mind and gives customers full control over how PII is retained and stored with the following features:

- Data access management
- Data encryption
- Data minimization
- Automatic data retention and deletion protocols

When a customer deploys SAFR, they should make full use of these tools to protect the privacy of their users. To help our customers we have put together best practices to ensure secure, privacy-conscious implementations: https://safr.com/safr-best-practices/.

**Consumer Perception**

Public perception of face recognition often centers around the idea that any use of facial recognition systems is a threat to individual privacy and that face biometric signatures can be hacked and/or used for harmful purposes without the subject's consent. This perception is possibly a consequence of

poor use of facial recognition technology during its infancy, improper use by a few bad actors, or a misunderstanding of the technology that is amplified through sensational media coverage.

As with all technologies, there are certainly ways face recognition can be abused. However, the weekly articles with dire warnings about the dangers of face recognition don't adequately convey the many ways this technology can be used with complete data security and only with opted-in individuals in order to improve safety and convenience.

We see examples of positive impact each week, but these stories are too often overshadowed by the negative noise. It's crucial that all computer vision, biometric, and facial recognition companies focus on positive use cases and help customers see how this technology can solve a range of human problems.

See examples of positive use cases: https://safr.com/facial-recognition-for-good/

### Ethical Use & Reducing Bias

There is well known racial and gender bias in many facial recognition algorithms as confirmed by studies from NIST and other independent evaluators. These biases are a direct result of poor training data and bias within product development processes. Deep learning algorithms are only as smart as the data on which they are trained and it's easy for developer bias to creep into algorithms if these unconscious biases are not addressed.

That's why it is critical to choose a facial recognition system that performs uniformly across faces of differing genders and skin tones and to commit to ethical use cases. Secure access is a perfect example of a positive use case, where all users are opted-in and consenting to being recognized. Selecting a facial recognition system that is low in bias will ensure a positive user experience and high-accuracy rate for all users of your face-based secure access system.

THE SAFR SOLUTION

#### Ethical Use & Reducing Bias

The SAFR development team set out with a goal to make the least-biased, most-trusted facial recognition system on the market. The SAFR algorithm was trained on a large, diverse, global data set of real faces and was not trained to recognize race. SAFR has been found to have consistent recognition rates across skin tone and gender in NIST tests, demonstrating the lowest bias of any globally available facial recognition algorithm.

SAFR is committed to advancing the ethical use of face recognition with our guiding principles: https://safr.com/the-safr-guiding-principles/.

# Face Recognition for Access Control

For face recognition to be confidently used in access control applications, developers and installers must ensure their solution meets the following criteria:

- High accuracy
- Able to recognize faces wearing protective masks
- Integration with legacy systems
- Robustness

## High Accuracy

Facial recognition solutions are consistently racing to achieve the highest accuracy levels. As this technology has advanced, accuracy rates have reached 99% for most enterprise solutions, while false acceptance and rejection rates are dropping to negligible levels.

Additionally, the quality of pictures received in cooperative access control applications are normally higher than any other use cases, making the job of the facial recognition algorithm simpler.

Cooperative Face

Wild Face

**200 px/m:** Minimum to perform face recognition with SAFR

**400 px/m**: High-accuracy face recognition with SAFR

**700 px/m**: Typical image quality acquired in secure access use cases (with fixed lens 1080p camera and 1.5m distance)

SPOTLIGHT

## Picture Quality

For any biometric solution, a quality template and biometric sample is key to achieving high accuracy and low false acceptance.

Access control applications are likely to have even higher facial recognition accuracy rates than passive monitoring use cases due to cooperation of the subjects. Enrollment is performed in a controlled environment with opted-in subjects providing high quality reference images. When access control systems are set up, cameras are placed within a maximum distance from subjects to ensure optimal pixel density (on average twice that required for high accuracy recognition).

THE SAFR SOLUTION

## High Accuracy

In independent NIST tests, SAFR's combined speed, accuracy, and low bias rates make it the best performing algorithm for live video face recognition — ideally suited for detection and recognition of wild faces.

99.87% accuracy rate for recognition of wild faces

<100ms average response time

Least biased globally available algorithm. <0.25% variance across tested racial groups

### Performance with Facemasks

With facemasks now a part of standard attire, it's crucial that any face-based biometric solution can detect and recognize even partially obscured faces. Facemasks reduce the amount of biometric information an algorithm can use to detect and correctly match a face. However, requiring a user to remove their mask at a secure access point introduces friction and increases the risk of virus transmission. Leading facial recognition providers understand this challenge and have invested in training their algorithms to detect and recognize masked faces.

THE SAFR SOLUTION

## Performance with Facemasks

When the COVID-19 pandemic began SAFR developers began re-training the algorithm with images of masked faces. SAFR 3.0 was released in fall 2020 with a new high sensitivity face detector that improved the algorithm's face detection rate for both masked and unmasked faces and dramatically boosted recognition accuracy for masked faces.

95% mask detection rate

98.85% recognition accuracy for masked faces

Widespread use of facemasks has made face recognition harder, but it has also sparked a wave of innovation that has made facial recognition algorithms that have chosen to adapt even faster and more accurate under a variety of real-world conditions.

### Legacy Integration

As facial recognition technology providers seek to be accepted in the access control industry, it's critical to consider how face recognition can fit into existing, well-established, and robust systems, processes, and technologies already used for access and visitor management.

In fact, security professionals often work with customers to customize their access control solutions in order to better protect their premises both from a technical and operational perspective. Access control systems include many capabilities and processes beyond the standard, "unlock a door" logic. For example:

- Employee database consolidation and auditing
- Integration with other security and safety systems (fire alarm, CCTV, IDS, etc.)
- Threat level management
- Emergency evacuation plan integration
- Visitor management integration
- Door monitoring (eg. door propped open)
- Emergency exit monitoring
- Tailgating monitoring
- Offline operations

Access control infrastructures can be extremely complex and hard to replace, therefore it is critical to choose a facial recognition solution that can integrate with the legacy system and complement existing infrastructure, not replace it.

THE SAFR SOLUTION

#### Legacy Integration

Thanks to the integration and customization capabilities mentioned earlier, SAFR is well positioned to integrate with access control systems. As an example, in the next section we will describe a typical implementation developed through the deep integration of SAFR with Genetec.

## Robustness

Despite the high level of accuracy reached by facial recognition solutions, some access control implementations — such as critical infrastructure, data centers, or financial institutions — may require additional layers of authentication.

Facial recognition solutions thus must be equipped with secondary authentication methods as well as anti-spoofing capabilities such as:

- Collaborative liveness: Access with an action that requires a response to a command (eg. smile to open)
- Two-factor authentication (2FA): Face + fixed or dynamic QR Code, face + card
- Three-dimensional liveness (eg. integrating with 3D cameras)
- Passive liveness (eg. using a standard 2D camera)

THE SAFR SOLUTION

### Robustness

With complete security in mind, SAFR has been developed with additional authentication solutions including liveness and anti-spoofing in order to equip security professionals to implement the most suitable options for their loss prevention and security plan. SAFR's presentation attack detection (also referred to as liveness detection or spoofing detection) works on any RGB video streams including IP-based surveillance, USB webcams, and cameras embedded in devices including ATMs, slot machines, smartphones, and tablets.

SAFR can detect spoofing attempts including faces printed on paper and displayed as static images or video on digital devices. Coupled with SAFR's alerting capabilities, intrusion attempts can be denied and security staff alerted to fraudulent penetration attempts in real time.

SPOTLIGHT

## Tailgating

One of the biggest concerns for security professionals when designing robust access control infrastructure is how to prevent tailgating — the passage of unauthorized or unrecognized persons into secure spaces behind authorized users. Several solutions and processes have been developed over the years to help prevent tailgating, namely IR/ laser sensors, man traps, turnstiles, and manual monitoring by standing security officers.

Although these solutions are often effective, they all require additional hardware, software, or human resources increasing the cost and complexity of the implementation.

Face recognition is uniquely suited to preventing and responding to tailgating without additional resources or complexity. Because the system is already detecting faces and seeking to match them to an authorized persons database, it will also detect if any unauthorized faces are in view at the secure access point. The face recognition system can be tuned to trigger notifications, alarms, or automated SOPs if unverified or unauthorized individuals are detecting loitering at a secure access point, attempting to gain access, or entering behind an authorized individual, making it by far the most secure and effective form of anti-tailgating.

If someone does successfully gain access behind an authorized individual, facial recognition systems make post-event analysis easy. Reviewing the event archive will show details about the event — who did the individual follow in, when did the event occur, what did the tailgater look like and what were they wearing, did somebody hold a door open — and provide the necessary information to respond to policy violations and prevent the incident from happening again.

## Additional Functionalities and Integration Possibilities

Another major advantage of using face recognition for access control is its potential to enhance the user experience when integrated into other security applications and processes. Beyond access control solutions, face recognition can be redeployed into:

- Integration between physical and logical access control
- Integration with video management systems
- Kiosk functionality and integration with standard visitor management systems
- Innovative visitor management and customer experience solutions (virtual assistant, robot concierge, etc.)
- Automated time and attendance capabilities

# SAFR-Genetec Access Control Case Study

## Requirement

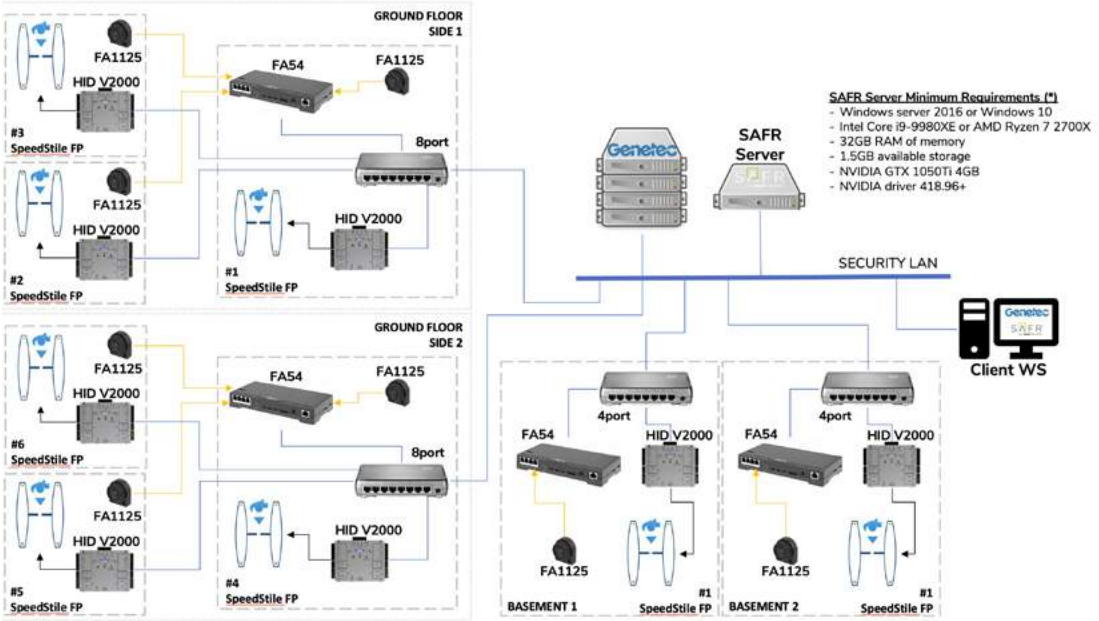
A commercial building using Genetec Security Center 5.7 wanted to upgrade their access control system to face recognition in order to ensure compliance with measures to reduce the spread of COVID-19.

The existing secure access point consisted of eight Gunnebo speed gates with biometric fingerprint readers and HID access control panels. The objective was to maintain the existing infrastructure to avoid additional costs and maintain current levels of accuracy and security while making the system touchless.

## SAFR Solution

Thanks to the off-the-shelf integration between Genetec and SAFR, the customer was able to retain their current infrastructure and smoothly transition from fingerprint biometrics to face recognition with the simple addition of an Axis pin-hole camera at each speed gate.

See a schematic of the application:




Thanks to a database integration between SAFR and Genetec Synergis, the customer was able to smoothly import the Genetec Synergis cardholder database details and images to SAFR in order to authenticate users at the secure access points, letting authorized individuals enter the building using just their face.

Operation of the Gunnebo speed gates did not change as the credential verification and decision-making process remained consistent within the access control system.

## Additional Capabilities of SAFR + Genetec Cardholder Database Integration

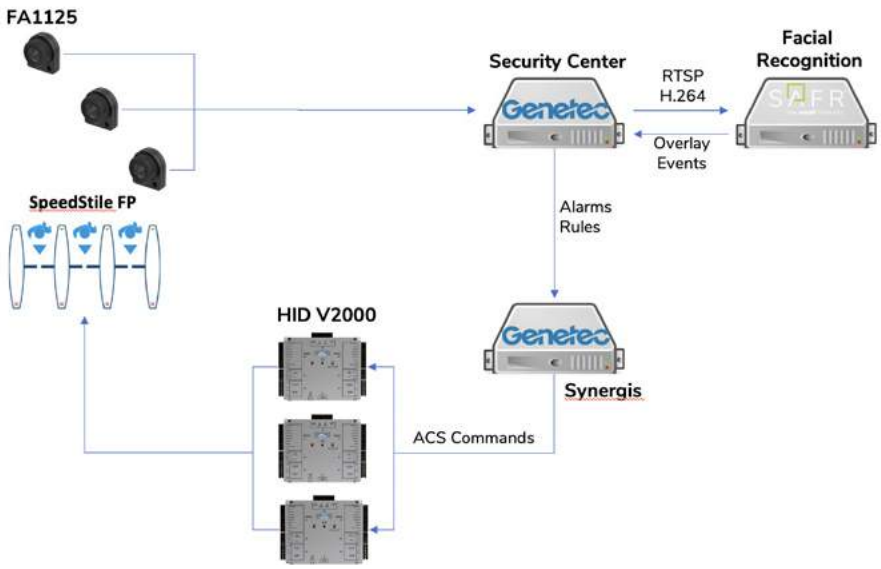
When integrated with SAFR, Genetec Security Center is equipped with several additional features with added value for use cases beyond secure access, should a customer choose to enable them:

**Video Overlays**: Identify people on camera instantly via visual cues, and categorize them as strangers, threats, unknown individuals, employees, VIPs, or other tagged individuals.

**Alarms & Notifications**: Customize real-time alerts to know immediately when persons enter, or exit, monitored areas. Customize actions to initiate building lockdowns or any number of security responses based on recognition events.

**Automatic Bookmarks**: Search timestamped metadata to review security footage — by time range, location, category, person type, or registered individual — for more efficient investigative or forensic work. Create custom bookmarks for common searches.

The workflow schematic shows how SAFR has been added without any modification to the existing environment or hardware, therefore maintaining the customer's configuration and policies.



## Conclusions

The rapid development of new machine learning capabilities combined with the continuous reduction of computing costs has made face recognition secure, accurate, and cost-efficient enough to become the norm in access control applications. In today's dynamic world, touchless applications offer additional benefits and peace of mind to users — and the shift caused by a global pandemic only accelerated the inevitable progress of face recognition's acceptance for commercial access control use.

It is possible to offer a truly frictionless user experience while providing enhanced safety and security. Face recognition offers a fast, automatic, secure, and seamless verification experience.

For more information:

Visit SAFR.com

Or email:

contactsafr@realnetworks.com