

The Metrics of Video Sensor Effectiveness

How small declines in accuracy can have a surprising impact on false positive ratios

By Jim Helman and Nicholas Imparato

Innovations move helter skelter in the field of security video software. The ascendance of video tools, particularly behavior analysis software, over the past few years has been astonishing. As always, the gap between expectations and reality in this environment needs to be addressed constantly. Nowhere is this more important than in understanding the logic and meaning of measures that speak to performance.

Metrics matter. Various vendor claims and user specifications are spun around the ideas of accuracy and false positives. However, these same specifications veil the fact that even a relatively small decrease in accuracy can have a significant impact on the number of false positives a system allows.

As an illustration, let's compare situations in which the accuracy rates are 99% and 90% in an access door application.

Above 99% Accuracy

In our first scenario, the overall accuracy rate is 99.4% and the misclassification rate is 0.6%, that is, less than one percent. Table 1 displays actual data from one test site where the total event count was 1,773. For the purposes of discussion, we've normalized the event count to 1,000.

The accuracy metric is derived from the sum of the normal behaviors that were classified accurately as non-violations (986) and the tailgating behaviors that were classified accurately as violations (eight). Notice that the system alarmed on 10 of the 1,000 door events, eight accurate alarms and two erroneous alarms. The number of erroneous alarms is the numerator in the false positive rate, or the false alarm rate—a

key metric for end users. The denominator is the total number of alarms. In this example, false alarms occurred about one-fifth of the time that the system alarmed (2 of 10), so they actually account for 20% of the alarms.

Notice as well the number of times the situation was declared normal but was not. This is a component of the false negative ratio. In this example, with a high accuracy rate above 99%, there were four missed detections per 1,000 events. These four incidents comprise one-third of the 12 times that tailgating actually occurred. That is, false negatives occur at a rate of about 33%.

Playing With the Numbers

Obviously, one can inflate or depress false positive and false negative scores by changing the denominator in the ratio—for example, by using the total event count. If measured this way, the system would look exceedingly robust, with a false positive rate of 0.2% (2 of 1,000) and a false negative rate of 0.4% (4 of 1,000)—hence the accuracy measure of 99.4%, as customarily defined.

At 90% Accuracy

Now let's see what would happen if we dropped the accuracy rate to 90%, as shown in Table 2 (p.16). The total number of real tailgaters is unchanged from the first example (12). This is a neutral assumption and a given—the number of tailgaters is what it is.

We presume that the system still misses 4 of the 12 violations. This means that the system is still generating a false negative rate of 33% when the number of real tailgating events is used in the denominator.

The number of events classified as normal that actually were normal would decline to 892 (900, from 90% accuracy, minus 8, the accurately identified tailgaters). The number of events classified erroneously as tailgating would rise to 96 (988 minus 892) from 2 in the previous case, an exponential deterioration in performance.

And that's the rub. The total number of alarms in this case would be 104 (1,000 minus 892 minus the 4 missed tailgaters). Thus, the false positive ratio would be 96/104, or more than 92%. The more lenient way to calculate the false positive ratio (96/1,000) would yield 9.6%, which along with the unchanged 0.4% false negative rate would give us the advertised 90% accuracy.

Table 1: 99.4% Accuracy

Actual vs. Detected Behaviors		Detected		Total
		Other/Normal	Tailgate	
Actual	Other/Normal	986	2	988
	Tailgate	4	8	12
Total		990	10	1000

Table 2: 90% Accuracy

Actual vs. Detected Behaviors		Detected		Total
		Other/Normal	Tailgate	
Actual	Other/Normal	892	96	988
	Tailgate	4	8	12
Total		896	104	1000

By the way, changing the number of missed detections, or the false negative ratio, won't change the outcome much, as long as overall accuracy is high. In this example, if we lowered the missed detections from four to zero, the numerator in the false positive ratio would be 100 (900 at 90% accuracy minus 12 equals 888; 988 minus 888 equals 100), yielding a false alarm ratio of 89% (100/112).

Where Is the Value?

How practical is a system with these kinds of error rates? Is an organization comfortable, for example, with the knowledge that every time it labels an actor as "in viola-

tion," it knows that it will be wrong 9 times out of 10, or even, as in the previous example, 2 times out of 10?

If the number of real violations stays the same, any drop in accuracy raises the false alarm rate significantly, no matter how it is computed. To achieve a low false alarm rate, a system for detecting a common event, such as a car entering a garage, does not need to be as accurate as a system detecting a rare event, such as the violation of policy at a facility with a high rate of policy compliance. Similarly, for situations in which "bad" behaviors occur infrequently, the overall error rate of the system has to be significantly less than the frequency of the "bad" behavior, or the false alarm ratio will be high. In practical terms, users' first priority is to diminish actual violations of policy. As "bad" events become less frequent, the accuracy of the system needs to rise in order to have value.

In short, there is practical value to understanding how metrics interact. They provide another data point that can be used when fashioning a security system that matches your approach to risk to an array of currently available tools and technologies. SIND

Jim Helman PhD was chief architect at SmartCatch, and Nicholas Imperato PhD is a research fellow at the Hoover Institution, Stanford University, and professor of management and marketing at the University of San Francisco. This article was prepared while both were consultants to NEC Laboratories and advisors to SmartCatch.



See Everything

Complete Situational Awareness with IPIX Technology

Replace several conventional cameras with one IPIX Network Camera to provide cost effective monitoring indoors or outdoors.



- Unobstructed full 360-degree field-of-view
- High resolution network cameras with 2.0 mega-pixel sensors
- Simultaneous viewers with independent navigation control
- View, record and playback full 360-degree high resolution video
- No blind spots, no moving parts
- Smart image management including motion detection
- Variety of enclosures and accessories

(888) 909-4749 or security@ipix.com



www.ipix.com

Circle Inquiry No. 208 or visit www.st-and-d.com and click on e-Inquiry