Make Some Alarming Moves

White Paper
exida
80 N. Main St.
Sellersville, PA
www.exida.com

April 2012

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Introduction

Most process plants strive to enhance their productivity and extend their asset life. One of the easiest and most effective ways to achieve such improvements is to address alarm system problems that undermine operator performance. After all, operators typically have more influence on product quality, raw material usage and energy utilization than any other production variable. Even at the most highly automated plants, yield, rate, quality and resource utilization often vary shift to shift because of operator impact.

Unnecessary alarms, such as ones that just provide information or don't require an action, reduce productivity, add stress, and take time away from managing the process. Transforming the alarm system from a hindrance to a help can significantly enhance operators' effectiveness. So, here, we'll describe how to create a program to optimize the alarm system by following the alarm management lifecycle defined in the ISA-18.2 standard "Management of Alarm Systems for the Process Industries" [1].

To determine how bad your alarm system is you need alarm rates and other key alarm system performance indicators to compare to industry benchmarks. Control system vendors and alarm management specialists offer excellent alarm analytic tools. However, you can obtain useful insights just by taking a clipboard into your control room and charting what happens in a typical 20-minute period. If your control room is like that of most plants without a formal alarm system management program, you'll probably see results similar to those in Table 1.

Times the alarm horn sounded	8
Times the operator acknowledged the alarm	8
Times the operator took action*	2
Number of standing alarms**	12
Highest priority observed	Warning (medium)
Operator used documentation?	No
Operator showed appreciable concern?	No

* Not counting silencing the horn, acknowledging the alarm or casually glancing at a control display.

** Acknowledged alarms that were on the list before you came into the room and that still were there when you were leaving.

Table 1: These results typify what happens during 20 minutes in a control room when alarms aren't properly managed

ISA-18.2 guidelines for incoming alarm rates state that an average of one alarm every 10 minutes is very likely to be acceptable, while the maximum manageable rate is two alarms per 10 minutes [1]. Our 20-minute sample averaged four alarms per 10-minute interval, which is beyond the maximum manageable rate. The operators acted on only two of eight new alarms and ignored 12 standing alarms, which also indicates the alarm system is performing poorly and causing undue operator interruption. Moreover, the operators acknowledged all eight alarms but only acted on two, meaning they appear to be deciding for each alarm whether it represents an abnormal condition and warrants an action (likely undocumented).

The Importance of Alarm Management

Poor alarm system performance has significantly contributed to many well-publicized industrial accidents. The consequences of such incidents coupled with new regulations like the U.S. Pipeline and Hazardous Materials Safety Administration's 49 CFR 195.446 (Section e focuses specifically on alarm management) and heightened insurance industry scrutiny provide compelling motivation to create a sustainable alarm system performance improvement program. Such a program can do much more than just avoid costly incidents — it also can add dollars to the bottom line. A properly managed alarm system should deliver positive measurable increases in operational performance regardless of shift.

Key elements for achieving operational benefits are:

- *Nuisance alarm elimination*. Ensuring that alarms are meaningful and relevant allows operators to focus on the process with minimum interruptions. The 80/20 rule is definitely true for most plants with no alarm management improvement program in place — a small number of fleeting, chattering or otherwise faulty alarm sources contribute to a majority of all alarms.

- *Alarm design review.* This can remove artificial barriers to alarm-free operation at higher performance levels. When examined closely during a process called rationalization, many alarms are found to be unduly conservative or sensitive, if not altogether unnecessary. Alarms should be implemented based on firm process knowledge such as root cause, process dynamics, operational limits, consequence of inaction, time needed/available to respond and an under- standing of the steps the operator must take to respond. This contributes to creating a useful alarm system that earns the operators' trust and empowers them to safely push past previous operating levels.

- *Operator access to alarm and process knowledge*. Alarm design information, including probable causes, potential consequences, recommended corrective actions and guidance on how to confirm the alarm's validity, can improve operators' performance. This knowledge often is locked up in the heads of a few senior operators. In a well-managed alarm system such details are made available to every operator, so each can recognize and correctly respond to process abnormalities faster and more consistently.

The Road to Recovery

The ISA-18.2 standard provides the blueprint for implementing an effective alarm management program. It outlines an alarm management lifecycle (work process) that can help eliminate or reduce alarm management issues. The insurance industry and regulators such as the U.S. Occupational Safety and Health Administration are expected to accept the standard as good engineering practice. For an overview of the standard and the alarm management lifecycle, see "Avoid the Domino Effect," www.ChemicalProcessing.com/articles/2010/033. html [2].

You can improve alarm system performance — and, in turn, operator performance — by implementing a program consisting of seven key steps:

1. Create an alarm philosophy document.
2. Measure alarm system performance, compare to key performance indicators (KPIs), and identify problem alarms.
3. Review the existing alarm system design and rationalize the alarms.
4. Document results in an alarm response procedure and train operators on how to respond.
5. Run revisions through the management-of- change process.
6. Implement alarm system changes dictated by rationalization.
7. Repeat periodically, starting at Step 2.

To control engineers, this overall process should look very familiar because it's very much like a continuous control loop. First you must measure performance, analyze how close you are to target, determine the necessary correction and then apply it to close the gap.

Create an Alarm Philosophy Document

Such a document is the cornerstone for developing an effective alarm management program. It establishes the guidelines for how to address all aspects of alarm management, including the criteria for determining what should be alarmed, roles and responsibilities, prioritization, management of change, and KPIs.

Alarm criteria. By ISA-18.2 definition, "an alarm is an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response." This definition helps establish the criteria to weed out invalid alarms during the rationalization process. Note that every alarm requires a response (other than acknowledging it). If the operator doesn't need to respond, then there shouldn't be an alarm. Other key criteria include:

- Every alarm should have a defined response.
- An operator must have adequate time to carry out the defined response.
- Each alarm should alert, inform and guide.
- The operator only should get alarms that are useful and relevant [3].

Roles and responsibilities. The document must clearly specify who handles each alarm-management-related task; this is critical to ensuring success and commitment of the necessary resources by management.

Prioritization. Alarm priority indicates criticality and which alarms to respond to first. To ensure consistency, the philosophy defines the prioritization methodology, which typically is based on the severity of the potential consequences and the time available to respond.

Management of change. The document must spell out processes for reviewing and authorizing alarm system changes, including whether operators can dis- able alarms or change their limits from the human machine interface (HMI).

Performance metrics. The philosophy defines KPIs such as the ones in Table 2.

Metric	Target	Action Limit
Average alarm rate per operator, alarms/day	<300	>600
Average alarm rate per operator, alarms/10 minutes	1–2	>4
Time alarm system is in flood, i.e., >10 alarms/10 minutes, %	<1	>5
Hours with >30 alarms, %	<1	>5
Average number of alarms out of service, %	<1	>5
Low priority alarms in total alarms, %	≈80	<50
Medium priority alarms in total alarms, %	≈15	>25
High priority alarms in total alarms, %	≈5	>15
Top ten most frequent alarms’ contribution to total alarms, %	<1–≈5	>20
Number of stale alarms, i.e., active for >24 hours, on any day	<5	>5
Number of chattering and fleeting alarms	0	>5

Table 2: Review performance against metrics such as these every month

Measure System Performance

Most alarm analysis packages provide reports that al- low easy comparison of measured performance versus metrics. A “bad actor” alarm report often will show that a few modules or tags cause a disproportionate number of alarms. Use such information as a starting point for improving alarm system performance.

Perform Rationalization

Systematically review existing or candidate alarms to ensure they meet the criteria established in the philosophy and to document their design. This is a team activity, similar to a hazard and operability study, involving at a minimum production/process engineers, control engineers and operators. Industry best practices spell out the steps in the process:

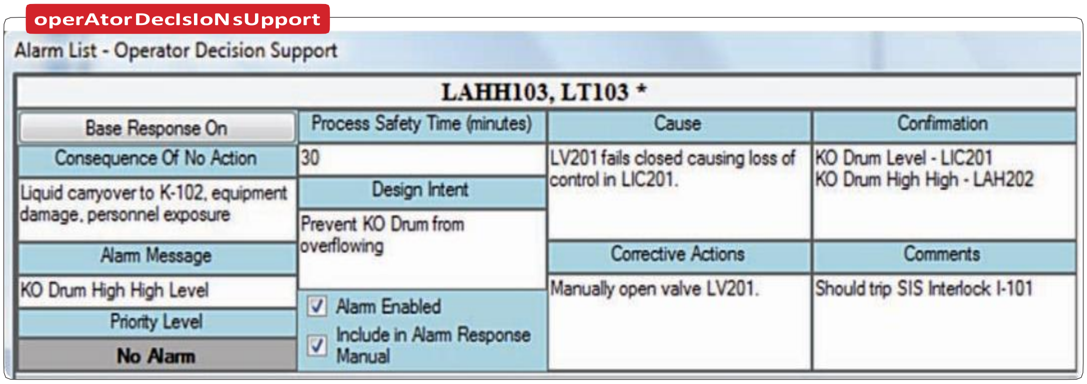
Check alarm validity. Ensure each alarm:

- indicates a malfunction, deviation or abnormal condition;
- requires a timely operator action to avoid de- fined consequences;
- is the best indicator of the root cause of the abnormal situation; and
- is unique, i.e., no other alarms also signal the same condition.

Any alarm not meeting these criteria can be re- moved, reducing the number presented to the operator.

Determine consequence of inaction. Identify the direct and immediate result of failing to manage the alarm. Consider only direct repercussions, not what could happen based upon a series of failures. For ex- ample, not dealing with a safety-critical alarm might lead to the trip of a safety instrumented system, not the hazardous event itself. Any alarm without significant consequences, e.g., that only generates another alarm, may not be needed.

Document cause, confirmation and corrective actions. Identify the most likely causes of the alarm and other process measurements the operator can use to confirm the alarm is real. Where an alarm response entails shutting down production, operators may want to verify the action truly is necessary before executing it. Spell out the action the operator should take, such as closing a valve or starting a pump, to correct the abnormal situation (Figure 1); acknowledging the alarm doesn't count.



operAtor DecIsIoN sUpport

Alarm List - Operator Decision Support

LAHH103, LT103 *

Base Response On	Process Safety Time (minutes)	Cause	Confirmation
Consequence Of No Action	30	LV201 fails closed causing loss of control in LIC201.	KO Drum Level - LIC201 KO Drum High High - LAH202
Liquid carryover to K-102, equipment damage, personnel exposure	Design Intent		
	Prevent KO Drum from overflowing		
Alarm Message		Corrective Actions	Comments
KO Drum High High Level	☑ Alarm Enabled ☑ Include in Alarm Response Manual	Manually open valve LV201.	Should trip SIS Interlock I-101
Priority Level			
No Alarm			

Figure 1: Providing relevant background information spurs correct response

Any alarm not requiring an operator response isn't valid and can be removed. Multiple alarm conditions sharing the same operator action may indicate redundant alarms, in which case one can be eliminated.

Document operator response time. Estimate the amount of time available between alarm activation and the last moment operator action will prevent the consequence. Compare this to the time needed by the operator to detect the alarm, diagnose the problem and complete all actions comprising the response. If time required exceeds time available, replace the alarm with an automated response (interlock).

Assign alarm priority. Evaluate the impact of the potential consequences in key areas like safety, environmental and financial, along with operator response time. The worse the repercussions and shorter the response time are, the higher the priority should be. This results in objective and consistent prioritization of alarms with highest priority assigned only to truly critical alarms.

Alarm classification. Record what category is ap- propriate for the alarm. An alarm classified as "safety critical" likely will have different requirements for training and testing frequency than the average process alarm.

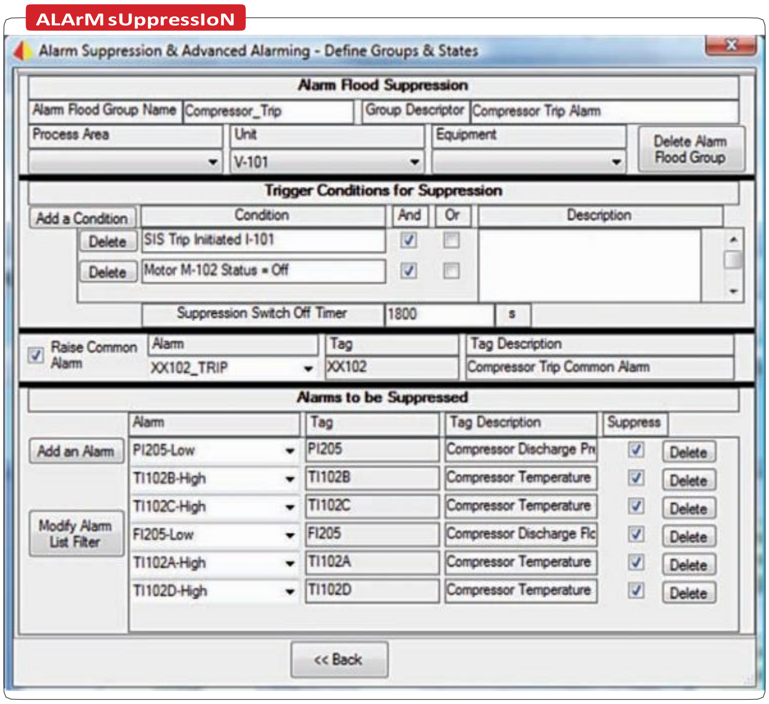
Determine alarm activation point (limit). Set limits far enough away from the consequence threshold that the operator has adequate time to respond but not so close to normal operating conditions that regular process variation triggers alarms.

A common mistake in creating alarms is to configure limits based on rules of thumb relative to the engineering range of the process variable — for example, configuring the limits for High-High, High, Low and Low-Low as 90%, 80%, 20% and 10% of range, respectively. This ignores the time the operator has to respond, the process variable's rate of change, the consequence threshold and process deadtime.

Verify other alarm-related settings and attributes. An alarm ideally should go off only once per event. Use deadband and on/off delays to reduce the number of times an alarm triggers for a single abnormal condition.

Proper application of deadband and alarm delays can minimize chattering alarms and also prevent problems during control system installation and commissioning.

Assess the need for special handling. Document the states, conditions, phases or products where the alarm limit or priority should differ from "normal" or the alarm should be suppressed (Figure 2). This ensures any alarm presented to the operator always is relevant



Alarm Flood Suppression

Alarm Flood Group Name: Compressor_Trip
Group Descriptor: Compressor Trip Alarm
Process Area:
Unit: V-101
Equipment:

Trigger Conditions for Suppression

Condition	And	Or	Description
SIS Trip Initiated I-101	☑	□	
Motor M-102 Status = Off	☑	□	

Suppression Switch Off Timer: 1800 s

☑ Raise Common Alarm

Alarm	Tag	Tag Description
XX102_TRIP	XX102	Compressor Trip Common Alarm

Alarms to be Suppressed

Alarm	Tag	Tag Description	Suppress
PI205-Low	PI205	Compressor Discharge Pr	☑
TI102B-High	TI102B	Compressor Temperature	☑
TI102C-High	TI102C	Compressor Temperature	☑
FI205-Low	FI205	Compressor Discharge Flo	☑
TI102A-High	TI102A	Compressor Temperature	☑
TI102D-High	TI102D	Compressor Temperature	☑

Figure 2: It's important to define situations where alarms aren't relevant and could lead to an alarm flood

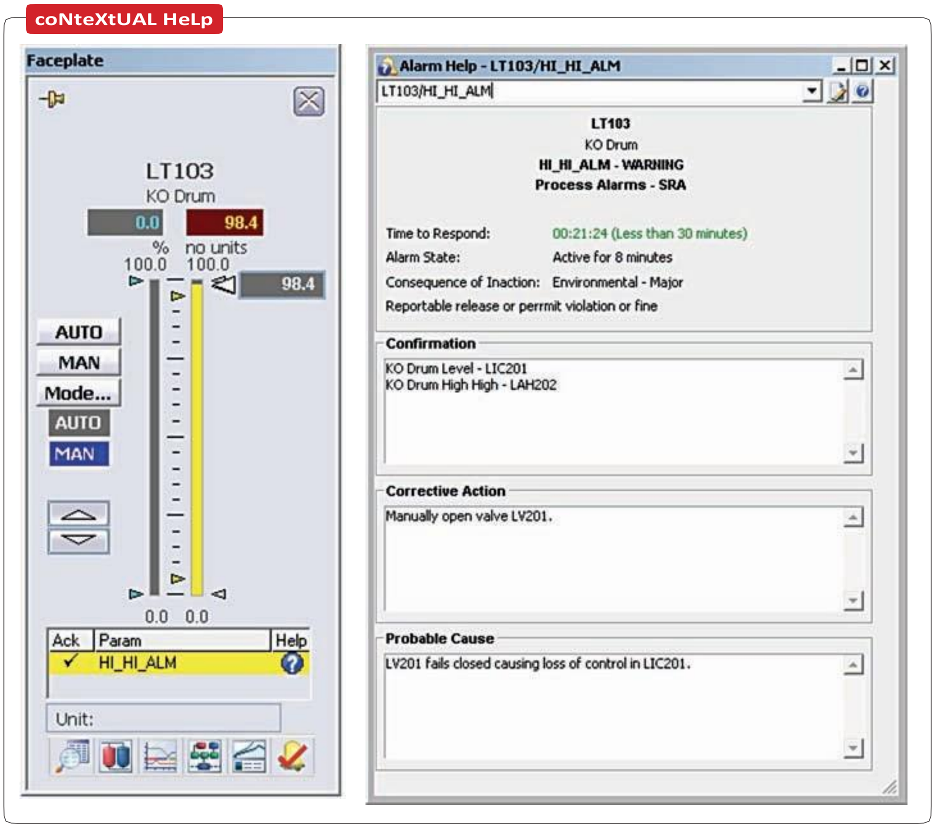
Record results in a master alarm database (MADB), which can range from a user-developed spreadsheet to a commercially available tool designed for the purpose. An effective tool can maximize efficiency by speeding completion of the overall process, saving money and reducing the time commitment of key personnel. It also helps produce consistent results from the first alarm reviewed to the last, even if team members change and the order of alarms reviewed varies.

A well-equipped rationalization team each day can complete 20 to 30 process tags (alarm sources) or more, representing 100 to 200 alarms. So, the choice of rationalization tool/MADB is important. Whether developed in-house or purchased, it should reduce dependence upon team member personality and training with mechanisms to enforce consistent review, apply philosophy criteria (priority setting as an example), facilitate management of change, allow similar alarms to be rationalized in mass and, ideally, enable efficient two-way exchange of alarm configuration data with the process control system.

Make Results Available

Alarms are only effective if operators know how to properly respond to them. So, provide operators with the information documented during rationalization (particularly the cause, consequence, corrective action, confirmation and time to respond). Such "alarm response procedures" can be used for operator training and integrated into the HMI to give operators on-line access, resulting in a quicker and more consistent response.

Ideally, a control system faceplate should offer direct access to appropriate alarm response procedures. Figure 3 shows a setup in which a click on the help icon adjacent to the alarm opened the alarm help window.



LT103
KO Drum
HI_HI_ALM - WARNING
Process Alarms - SRA

Time to Respond: 00:21:24 (Less than 30 minutes)
Alarm State: Active for 8 minutes
Consequence of Inaction: Environmental - Major
Reportable release or perrmit violation or fine

Confirmation
KO Drum Level - LIC201
KO Drum High High - LAH202

Corrective Action
Manually open valve LV201.

Probable Cause
LV201 fails closed causing loss of control in LIC201.

Ack	Param	Help
✓	HI_HI_ALM	?

Figure 3: Clicking on icon next to alarm on faceplate opens help window

Manage Change

Run any alarm configuration changes captured during the rationalization process through the management-of-change process before approving their implementation. The level of review may differ depending upon the type of change and the alarm's classification. For example, adjusting the limit of a safety-critical alarm may require a more-thorough review and approval process than altering the deadband of a typical process alarm. Update the MADB to reflect any changes made in the alarm system configuration so they are kept in sync.

Implement Alarm System Changes

Create a strategy to manage moving the new alarm settings established during rationalization to the control system alarm configuration. You don't have to manually enter the settings — commercially available rationalization tools can transfer all parameters, including alarm limit, priority, deadband and on-delay, and automatically update the control system.

Before bringing the alarm system changes online, ensure that adequate testing and opera- tor training has been carried out. This can include reviewing the online alarm response procedures, which the rationalization tool can create automatically.

Repeat Regularly

Alarm management is a never-ending activity. Plan to spend some time every month reviewing alarm system performance, identifying new bad actors and evaluating how things have changed during the month. Work your way through the entire alarm configuration one subsystem at a time, starting with those most critical.

Help Your Operator and Bottom Line

When designed and implemented properly, alarms can help operators keep your plant running safely and within normal operating conditions. However, if alarms instead serve as distractions or nuisances, then operator performance will suffer. Taking steps to ensure your alarm system performs well can lead to improved operational excellence and reduced risk that process abnormalities will escalate to major events. The ISA-18.2 alarm management lifecycle provides a framework for addressing common alarm management problems.

References

1. "Management of Alarm Systems for the Process Industries," ANSI/ISA ISA18.00.02-2009, ISA, Research Triangle Park, N.C. (2009).
2. Sands, N.P. and T. Stauffer, "Avoid the Domino Effect," p. 16, *Chemical Processing*, (February 2010), online at www.ChemicalPro- cessing.com/articles/2010/033.html.
3. "Alarm Systems — A Guide to Design, Management and Procurement," 2nd ed., Engineering Equipment & Materials Users' Assn., London, U.K. (2007).

Revision History

Authors: Todd Stauffer, Kim VanCamp

Reprinted with permission from Chemical Processing, April 2012.

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

  - PHAx™ (Process Hazard Analysis)
  - LOPAx™ (Layer of Protection Analysis)
  - SILAlarm™ (Alarm Management and Rationalization)
  - SILect™ (SIL Selection and Layer of Protection Analysis)
  - Process SRS (PHA based Safety Requirements Specification definition)
  - SILver™ (SIL verification)
  - Design SRS (Conceptual Design based Safety Requirements Specification definition)
  - Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
  - PTG (Proof Test Generator)
  - SILstat™ (Life Event Recording and Monitoring)
- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com