Results of the SANS SCADA Security Survey
SANS SCADA and Process Control Security Survey

February 2013
A SANS Whitepaper
Written by: Matthew E. Luallen
Advisor: Barbara Filkins

Survey Participants  PAGE 2
Risk Awareness  PAGE 4
Their Security Programs  PAGE 7
Recommendations  PAGE 16
Executive Summary

SCADA system operators are keenly aware of the risk to their systems, according to a survey of nearly 700 participants conducted by SANS Institute. In it, 70% consider the risks to their systems to be high to severe, and 33% suspect they may have had incidents.

This comes as no surprise to SANS and this survey's sponsors. SCADA and process control systems are opening multiple connections to external networks and the Internet, and are being administered over handheld mobile devices owned by system administrators. SCADA devices were never intended to be operated remotely and over the Internet, and therefore have little or no native security. Because of the sensitive nature of these systems’ operations, patching, updating and securing these systems and their underlying operating systems is difficult.¹

In other words, without protection, these systems are sitting ducks. Indeed, numerous reports reveal SCADA systems are under increasing attack,² and demonstrate multiple vulnerabilities. The US ICS-CERT responded to 198 reported cyber incidents against control systems in fiscal year 2012—41% of those against the energy sector. Of those incidents, 23 were the results of a targeted industrial control system (ICS) spear-phishing campaign, while some were the result of infected USBs in use by system administrators. The report also indicated that numerous control systems with IP addresses connected directly to the Internet were riddled with vulnerabilities exploitable from the web.³

To find out how organizations are dealing with this risk, SANS has just completed an in-depth survey to determine their risk awareness and security practices. Respondents indicate a variety of concerns, chief among them being malware such as Stuxnet and its related strains, insider threat, and hacktivism/sponsored attacks.

The survey also shows that operators are taking steps toward broader protection capabilities: More than 50% have patching and update practices. Those that use protections are doing so through access controls, monitoring and log analysis of their network devices, firewalls, and computer assets running the control systems. Unfortunately, at this time they seem unable to monitor the PLCs, terminal units and connections to field equipment due to lack of native security in the control systems themselves.

Survey Participants

The survey sample spanned a wide range of sectors, all of which have significant responsibility to maintain and secure their systems. The categories selected for inclusion in this survey were based on the 18 critical infrastructure sectors outlined in the current U.S. National Infrastructure Protection Plan (NIPP) (see Figure 1).  

What is your organization’s primary industry?

- Chemical Production
- Engineering Services
- Energy/Utilities
- Hydro Production/Wastewater
- Healthcare/Pharmaceutical
- High-Tech Production
- Oil and Gas Production/Delivery
- Other Manufacturing
- Transportation
- Water Production and Distribution
- Wastewater
- Other (Please specify)

Figure 1. Industrial automation spans a wide range of industries.

The “Other” category (39%) was by far the largest. Interestingly, respondents used more than 100 other categories including mining, government, defense, HVAC/building automation, shipping and logistics, telecommunications, education and industrial software development. As expected, Energy/Utilities (23%) was well represented, as were a variety of other industries.

Respondents also represented a variety of organizational sizes, half of them being from global and large multinational enterprises, and the rest from large, small and medium enterprises, as illustrated in Figure 2.

How large is your organization?

- Global 200
- Multinational enterprise (2000 or more employees)
- Medium enterprise (1000 to 1999 employees)
- 500 to 1999 employees
- 100 to 499 employees
- Fewer than 100 employees

Figure 2. Organization Size

The largest response group (51%) characterized their role(s) as a security administrator/analyst, followed by network operations and system personnel. Respondents were allowed to select more than one role in this survey, and many did. Notably, besides these categories, the respondents covered a cross-functional group ranging from average business users, auditors, managers and engineers, with other specific engineering, technology, auditing, and administrative professions also represented in the “Other” category (see Figure 3).

It is also interesting to note that only 5% of the respondents listed themselves as consultants employed in this industry segment. This strong showing of employee-based IT workers may be because of the need to have stricter control over personnel that interact with these systems, given the sensitive nature of their functions. In the “Other” column, multiple technology and IT security roles were represented, as well as such roles as process software engineer, smart grid integrator, division manager of control system operator, researchers and penetration testers.

![Figure 3. Respondent Roles](image-url)
Risk Awareness

Across this varied group of responses, risk awareness is strong. Nearly 70% of respondents believe the threat to be High (53%) to Severe (16%), as illustrated in Figure 4.

This response seems appropriate, considering that nearly all industrial automation revolves around critical business and government functions. And, since Stuxnet, respondents and industry professionals have been exposed to more public information and news around cyberthreats and incidents involving control systems. Recent reports from Computer Emergency Response Teams (CERT), government agencies and asset owners confirm an escalating risk of cybersecurity events, specifically to the electric sector.5

Vectors of Most Concern

The survey indicates that the top threats identified by the respondents are internal, advanced zero-day malware such as Stuxnet or Flame, and external threats from hacktivists, terrorists or governments, as shown in Figure 5.

Given all the media around Stuxnet, Aurora and other malware families targeting control systems using multiple vectors, these responses are logical. However, the recent and continued spear-phishing campaign to gain remote access to control systems indicates that users themselves are still under attack. So, in addition to technologies to fill the security gaps in control system networks, end points must be protected against these attacks. In addition, operational and maintenance personnel must continually be educated on the threats they, personally, can bring to their systems.

In a separate question, 82% of participants indicated they are or will be providing cybersecurity education to employees in the next 12 months. Education is helpful, but only if it teaches on useful topics.

Training should include specific operational topics on spear-phishing, zero-day activities and managing internal threats. Survey respondents indicate that they are concerned with phishing scams, which makes sense given that many of the attacks against these controls still rely on some internal person doing something, such as inserting a USB drive, remotely accessing equipment or clicking a link or attachment. Phishing scams can also lead to industrial espionage, so there is a lot of crossover between the types of threats they perceive.

**Who’s Been Hacked**

The survey results indicate that organizations either do not know they’ve been compromised or they are not being compromised as much as has been suspected. Our guess is the latter. While 20% of respondents have detected compromises among their control system cyber assets or control system network, another 8% believe they have been compromised but can’t prove it, and 13% don’t know. With 40% indicating they have been, suspect they’ve been or don’t know if they’ve been attacked, the number is as expected (see Figure 6).

![Figure 6. Control System Breaches](image)
Those 13% that don’t know whether they have been compromised have likely been infiltrated because they have no visibility; and even some of those who thought they have not been breached may have been infiltrated, but still don’t know it. So, it is likely that the percentage is higher still. We do know that the US ICS-CERT responded to 198 reported cyber incidents against control systems in fiscal year 2012, as reported earlier in this paper.

Ultimately, security is about detecting and responding to attacks. With 40% of the respondents stating that they have been compromised or that they don’t know if they have, protecting the systems and assuring detection and attribution are serious challenges that must be addressed with awareness, policy and technical controls.

Security is the long-standing process of monitoring the results of security controls, investigating for event(s) and responding to actual intrusions.

Those who did have incidents were asked to answer another question about the frequency of their incidents. In the past 12 months, nearly 10% of the respondents have detected an intrusion and more than 20 entities have suffered three or more intrusions, as shown in Figure 7.

As defenders add more security, they detect attacks that they hadn’t been able to detect in the past. Unfortunately, as organizations add more defenses, attackers identify more weaknesses to exploit and, therefore, stay ahead of protections. Considering higher risk awareness, growing international tensions and limited attribution capabilities in most SCADA environments, it is reasonable to predict that the number of identified infections will continue to increase in coming years.
The top three drivers identified by respondents for securing their systems align with the operational criticality of the industrialized systems. These drivers are: prevent service interruption, ensure the health and safety of employees and prevent damage (see Figure 8).

Conversely, it is a bit alarming that “Securing connections to external systems” was rated so low. This is the very paradigm that is creating the risks to these systems in the first place. However, because the ranking only allowed three choices, these less critical objectives would naturally fall lower on the ranking than the three primary objectives.
Areas of Risk

When it comes to the assets of most concern, respondents prioritized computer assets—Human Machine Interface (HMI), server, workstation—network devices and then embedded controllers as their primary sources of concern, as shown in Figure 9.

The top concern selected is computer-based workstations running the controllers rather than the embedded controllers running the industrial systems. While they may be monitoring the workstations, the embedded controllers should also be protected, because they were also heavily targeted by Stuxnet and its malware kin. Unfortunately, most organizations cannot provide security capabilities—such as authentication, authorization and accounting—for these controllers because they typically do not have native security controls. Control system vendors are improving their products, and some are working with IT security vendors to layer on the best controls. But these systems are designed to run for years and are not replaced very often.

Figure 9. Components of Concern

---

It also impossible to ignore the idea that connections between control systems and field systems are of lowest concern. Most control networks have connections to other physical areas of less trust, and these connections may provide an easy way for attackers to infiltrate and disrupt services or worse. Additionally, the protection of physical access systems and integration of those systems into the physical and cybersecurity response program is critical. Its low ranking on the survey may be attributed to the roles of the respondent: no physical security professionals responded to this survey.

When it comes to monitoring control systems (collecting log data), answers align with what respondents also consider to be most risky. These include computer assets hosting the controllers (80%), network devices and firewalls (81%), and connections to other internal systems (50%). Physical access systems are also monitored by 55% of respondents (see Figure 10).

Control system communication protocols such as Modbus, DNP3, Profibus and ICCP were monitored by only 35% of the respondents. This is of critical concern because the protocols themselves are natively insecure, allowing anyone with the ability to communicate with the device to control the device’s function. This number should be 100%.

Of the 17 “Other” responses, six answered “None,” or “N/A,” and one indicated they only monitor for performance. Video cams and protection systems were also listed.

Historically, with physical and operational security, and now with cybersecurity, the challenge of monitoring for and responding to malicious activity is daunting. The computers that support control systems are responsible for control functions that cannot be carried out by a human being. These systems are only as intelligent as the programming with which they are directed and can be coerced to do anything an administrator user tells them to.
In control systems, the actual components and communication protocols are the weak security link and the hardest to secure. The embedded devices (e.g., PLCs, RTUs, MTUs, meters, controllers) and communication protocols need to be altered by the industry to natively support security capabilities. Many initiatives to provide secure protocols are underway through the IEC TC57 WG15 on security standards for data communications such as IEC 60870-5, Secure DNP, Secure ICCP (IEC 60870-6), and IEC 61850 published as IEC 62351. As stated earlier, control system vendors and partners are working on this, but the time it takes for organizations to swap out their systems is measured in dozens of years, not in cybercrime time.

Our advice is to start with simple controls to isolate the embedded systems and then identify approved communications patterns. Afterward, enable an intrusion detection system to monitor and alert for communication patterns that are not approved and hire onsite staff to respond to these alerts. Such steps are costly, but the risk of doing nothing is unimaginable.

**Personnel**

The survey shows that responsibility for security is spread among many key players. Information security officers (52%) lead the pack, with the owners/operators for the system coming in a close second (49%), as shown in Figure 11.

![Figure 11. Responsibility for Security of Control Systems](http://en.wikipedia.org/wiki/IEC_62351)
The results may be skewed because of confusion in definitions. For example, there is a difference between who is responsible and who is accountable. Responsible parties are the ones who need to maintain the security that is agreed upon by the party that is accountable. Accountability and responsibility are outlined in the NERC CIP mandatory cybersecurity and reliability standards. It may be necessary to have similar mandatory standards in other critical infrastructures and control system environments.

The question is also a bit tricky to answer because control systems can easily span across a variety of areas in the business. For instance, the power grid has generation, transmission, distribution, and a variety of other independent and collective control systems. The same entity may also have physical access control systems and building management control systems. If the responsibility lies solely with the independent owner and operators, then the sharing of information among other operating peers and accountable parties may never occur.

**Standards-Driven**

The most commonly used standard is the NIST Guide to SCADA and Industrial Control Systems Security (40%). Other highly referenced cybersecurity standards include the 20 Critical Security Controls (34%) and NERC CIP (30%), as shown in Figure 12.

![Figure 12. Cybersecurity Standards Mapping](image-url)

---

10 [www.sans.org/critical-security-controls/](http://www.sans.org/critical-security-controls/)
11 [www.nerc.com/page.php?cid=2%7C20](http://www.nerc.com/page.php?cid=2%7C20)
The NIST Guide to SCADA and Industrial Control System Security is the most popular standard. This is alarming because the guide was in the revision process in 2009 and then dropped from the update process when confusion set in between the NIST guide and NERC CIP requirements. This guide has not been updated since then and is outdated, and therefore, severely lacking in specifics to control system environments and the lessons learned gleaned from NERC CIP. The much more specific NERC CIP version 5 requirements were approved by NERC Board of Trustees in November 2012, and are awaiting filing with FERC.\(^\text{12}\) The updated requirements provide greater direction on change management and monitoring and may serve as a better industry standard.

In the meantime, the 20 Critical Security Controls are gaining momentum and may become more popular than the NIST and NERC guidelines in the future, based on a GCN report.\(^\text{13}\) The control specifics simply need to be reworded to match the specifics for SCADA and control system environments.

Of the 26% of respondents that selected “Other,” nearly half indicated either they didn’t map their control systems to any standards or they didn’t know which ones to map to. As defined in the NIST PRISMA IT Security Maturity model,\(^\text{14}\) “if no cybersecurity procedures are used for systems, then the current state of the environment is unknown and the organizations are at a maturity level of 1 in NIST’s five-level maturity model.” The “Other” popular models were ISO 27001, NRC, DoD and Australian security standards, along with many responding that either they didn’t know, “N/A,” or “None.”

**Procurement Practices**

The good news is that 29% of respondents have a clear list of security requirements for their control systems, and 37% map compliance to as many standards as possible. Alarmingly, 17% still do not have security requirements when it comes to acquiring control system technologies, while another 12% appear to rely only on vendors for their SCADA security (see Figure 13).

\[\text{Figure 13. Cybersecurity in the Automation Systems Procurement Process}\]


14 [http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html](http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html)
These vendor-built systems are beginning to address the security risks that their connected products are posing. A key way to affect change control system protections is through more secure products, well-supported security updates for aftermarket solutions, and support for underlying operating systems, which control system vendors are working to provide. As organizations do acquire products, they should question the vendor’s role in maintaining system security, including updates, patches and compatibility with third-party security tools.

**Patches and Updates**

Vendor patches are also being applied. The good news is that more than half of respondents (52%) are installing vendor patches on a regular basis, 25% patch in a batch process, and another 4% are patching virtually to avoid downtime, as show in Figure 14.

![How are patches and updates handled on your critical control system assets? (Choose the most applicable)](chart)

We did not ask how they validate vendor patches, which could be asked in a follow-up survey. Organizations starting to undertake patching of their control systems and underlying operating systems must have a validation process in place to make sure that the patches don’t introduce new risks or break processes. This is why we asked the question about virtual patching, which is used by 4% of respondents.

It was also surprising that the most common response was not, “We layer on additional controls instead of patching.” Perhaps this is because we included the phrase “instead of patching.” If we’d replaced the word “instead” with “including,” we might have a completely different answer. And yet, when you look at the next section, you’ll see that there is much room for growth in the use of tools and processes deployed by respondents.
Tools and Processes

Organizations are reaching out for a variety of controls, the top choices being access controls, employee education, asset identification, monitoring and log analysis and antimalware. Interestingly, gateways to prevent direct access between the control system network and the rest of the network was of low priority, as shown in Figure 15. This is surprising, given this technology is one of the earliest controls, and separation is cited in NERC CIP and the 20 Critical Controls as highly effective.

Respondents chose assessment/audit as their largest growth area over the next 12 months, followed by application whitelisting and more monitoring capabilities.

When taken in combination, the emphasis of assessment and audit, application whitelisting, and monitoring and log analysis activities is a move toward continuous monitoring for compliance as outlined by NIST15 and the 20 Critical Security Controls.16 This includes application-layer analysis to detect malicious changes, such as, “Were there any changes (or attempted changes) made to Active Directory outside the scope of change management policies or normal employee behaviors?”

The continued emphasis on assessment and audit, application whitelisting, and log monitoring and analysis activities are good next steps by asset owners to reduce risk, improve compliance and apply threats to their actual systems and versions.

---

16 www.sans.org/critical-security-controls/
In Case of Emergency

When it comes to event response, most organizations prefer to handle their problems internally, as noted in Figure 16.

Respondents rely on internal resources (55%) and consult with government organizations (41%) rather than contact external consultants. This is in keeping with this survey’s demographics section, in which most organizations rely heavily on internal staff rather than consultants. Asset owners typically do not use peers (19%) or engineering consultants (10%) for initial consultation in the case of an event involving their control system assets.

It’s right to keep control system secrets close to home, working with in-house staff as much as possible. However, peers and consultants can provide valuable external threat intelligence and other insight into how widespread the attacks are and what impact the attacks have on operations.
Key takeaways and advice based on this survey’s findings include the following:

1. Layered controls will be incredibly important, particularly until organizations are able to swap out their older SCADA technologies and their underlying operating systems with more stable, secure technologies now on the market and in development.

2. Patch, update and test for vulnerabilities through regular vulnerability scans and penetration testers.

3. Visibility is vital. Monitor your control system networks’ inbound and outbound connections, remote access, operating systems supporting the devices, machine-to-machine calls and endpoint actions such as USB downloads.

4. Monitoring should be accompanied by means that make sense of what the data is telling you. This may require a new mindset of “thinking like an attacker” and understanding what indicators of compromise might look like in your environment. Today, this is difficult, even in nonSCADA networks. So, watch for tools that can provide deep analysis, and add the right amounts of context while applying your own real-world intelligence rather than just providing reactive signatures.

5. Automate where possible and appropriate. This is a key tenet of the 20 Critical Security Controls and will reduce human-induced errors.

6. Spread risk management responsibilities across the organization, with accountability residing at an upper layer so that layer has authority to effect change in the system if and when necessary. Get buy-in at the highest levels you can.

7. Education must be integrated into the operating environment, must continue to evolve as situations change, and should encompass phishing, BYOD, insider threat and other contemporary issues.

8. Continue to educate the community at large. At the Hawaiian International Conference of System Sciences (HICSS) in January 2013, academic professionals presented papers on the topic of developing control system cybersecurity courseware. US-CERT is making special reports related to the control system community, and NERC continues its public outreach.

---


Conclusion

As control systems reach the outside world, their operators are increasingly aware of new risks these connections have opened. Information about the systems they operate is publicly available for tools such as Stuxnet to take advantage of vulnerabilities in specific control system technologies they decide to target.

While the security challenges reported in this survey are substantial and pervasive, the results demonstrate that operators are aware of the risks they face and are actively engaged in efforts to mitigate them. Success in achieving these requirements will occur only after asset owners and operators understand the requirements and the requirements are subsidized and implemented by the industry, vendors and integrators.
About the Author

Matthew E. Luallen is cofounder and president of CYBATI, a critical infrastructure and control system cybersecurity consulting, awareness and training company. He has written, consulted and trained extensively on process control and SCADA security issues and continues to work with electric utilities in the U.S. and Canada on the NERC CIP reliability standards. He has also presented and consulted on ICS cybersecurity within critical infrastructures to the FBI InfraGard, FBI, ISA, NERC RROs, USSS, NNSA, DOE National Labs, U.S. Army Central Command, FAA, European Union, RCMP, and at the request of specific asset owners. Mr. Luallen holds a bachelor’s degree in industrial engineering from the University of Illinois-Urbana, a master’s degree in computer science from National Technological University and is a 13-year Cisco Certified Internetwork Expert (CCIE). He serves as adjunct faculty for DePaul University’s capstone cybersecurity and control system courses, as a certified instructor for Cisco Systems and as a certified instructor for the SANS Institute. He is also the author of a hands-on, control system cybersecurity course promoted by CYBATI.

SANS would like to thank its sponsors:
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Security West 2018</td>
<td>San Diego, CAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2018</td>
<td>Melbourne, AU</td>
<td>May 14, 2018 - May 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Reston Spring 2018</td>
<td>Reston, VAUS</td>
<td>May 20, 2018 - May 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2018</td>
<td>Amsterdam, NL</td>
<td>May 28, 2018 - Jun 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta 2018</td>
<td>Atlanta, GAUS</td>
<td>May 29, 2018 - Jun 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Washington DC</td>
<td>Crystal City, VAUS</td>
<td>Jun 08, 2018 - Jun 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud INsecurity Summit - Austin</td>
<td>Austin, TXUS</td>
<td>Jun 11, 2018 - Jun 11, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit and Training 2018</td>
<td>Munich, DE</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Crystal City 2018</td>
<td>Arlington, VAUS</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo June 2018</td>
<td>Oslo, NO</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2018</td>
<td>Manila, PH</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2018</td>
<td>Minneapolis, MNUS</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vancouver 2018</td>
<td>Vancouver, BCCA</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2018</td>
<td>Canberra, AU</td>
<td>Jun 25, 2018 - Jul 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Charlotte 2018</td>
<td>Charlotte, NCUS</td>
<td>Jul 09, 2018 - Jul 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Bangalore 2018</td>
<td>Bangalore, IN</td>
<td>Jul 16, 2018 - Jul 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Malaysia 2018</td>
<td>Kuala Lumpur, MY</td>
<td>Jul 16, 2018 - Jul 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh July 2018</td>
<td>Riyadh, SA</td>
<td>Jul 28, 2018 - Aug 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pittsburgh 2018</td>
<td>Pittsburgh, PAUS</td>
<td>Jul 30, 2018 - Aug 04, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 in Thai 2018</td>
<td>OnlineTH</td>
<td>May 07, 2018 - May 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>