# ARES COMMUNICATOR

Information for Scott County Amateurs

*June, 2016* | Accurate, Reliable Emergency Communications for our Community | *Volume 16, Number 6*


## Handiham Pioner SK

By: Patrick Tice, WA0TDA, HandiHams-*Retired*

It is with a heavy heart that I pass along the news that Sister Alverna O'Laughlin, WA0SGJ, has become a silent key on the 30th of May, 2016. She died among friends at Assisi Heights, the Franciscan residence in Rochester, Minnesota where she had been retired since 2007. She was 84 years old - and many of those years we knew her as "Sweet Grape Juice", WA0SGJ, her ham radio callsign suffix.

Sister Alverna O'Laughlin, WA0SGJ

Sister Alverna joined the fledgling "Handihams" in the earliest days when founder Ned Carman, W0ZSW, came up with the idea of sharing his hobby of Amateur Radio with people who had disabilities. Ned enlisted the help of a group of local nuns, the Sisters of St. Francis, on April 30, 1967. Although their first action was as weather watchers during a thunderstorm that passed through Rochester that day, the Sisters were committed to helping Ned with his new project, and several received their licenses. Among them was Sister Alverna O'Laughlin, WA0SGJ, who would eventually become the Educational Coordinator for the Handiham System at Courage Center in Golden Valley, MN.

It was at Courage Center in 1991 that I met Sister Alverna when I started a new job as the manager of the Handiham program. Her kindness and patience lifted me up, helping me to learn how to work with our Handiham members - just as she

*cont'd col. 2*

worked tirelessly to help those around her succeed and reach their goals. Think about how many people joined the ranks of Amateur Radio over the decades, thanks to the guidance and encouragement - and hard work - of Sister Alverna! She knew that radio would open a line of communications between those she taught and the rest of the world. Making friends on the radio, learning the math and science of electronics, and striving toward goals were all things that would make the lives of Handiham members better.

Sister knew that.

She was on a mission.

You were going to succeed in earning your ham radio license.

And she was right.

"73", Sister Alverna. You are at peace now and your lifetime of good work lives on in all of the thankful people you helped.

*BREAK - OVER*

**Congratulations 2016 Graduates!**

## ARES Activities

**Weekly Net Monday 7 PM 146.535 mhz (s)**

**Breakfast Saturday, July 9th**

**Digital Monday, July 11th**

### ARES Nets

MN ARES Phone Net
6:00PM Sunday Freq: 3.860 mhz

ARRL MN Phone Net
12:00p, 5:30p CST Daily Freq: 3.860 mhz

ARRL MN CW Net
6:30p, 9:50p CST Daily Freq: 3.568 mhz

**NETS WITH OUR NEIGHBORS**

| | | |
|---|---|---|
| North Dakota: | Daily 3.937 mhz | 6:30pm |
| South Dakota: | Daily 3.860 mhz | 6:00pm |
| Wisconsin: | Daily 3.985 mhz | 5:30pm |
| Iowa: | Daily 3.970 mhz | 12:30/5:30pm |


The ARES COMMUNICATOR is published for the benefit of Amateur Radio Operators in Scott County and other interested individuals.


EDITOR: Bob Reid, Scott County Emergency Coordinator
Snail Mail: 13600 Princeton Circle
Savage, MN. 55378
E-Mail: N0BHC@aol.com
Phone: Home 952-894-5178 Portable 612-280-9328

# Summer Events '16

Grab your HT and have some fun volunteering for a Public Service event this summer! You get the chance to use your communications skills to benefit the community and meet some new Hams. Hey, there might even be a "Free Lunch" thrown in for good measure.

Check out the events listed below and volunteer for a couple hours of ham radio fun!

### Monday, July 4th - City of Richfield

4th of July Parade
Staging at 11 AM at Richfield PD
Parade 12-Noon to 2:30 PM.

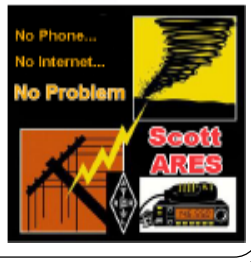
If you are interested in any of these events, please RSVP to KC0QNA: email kc0qna@yahoo.com
Phone 612-578-7561

*BREAK - OVER*


## Scott County ARES Contacts

Emergency Coordinator
Bob Reid N0BHC
13600 Princeton Circle
Savage, MN 55378
952-894-5178
N0BHC@arrl.net

Asst Emergency Coordinator
Chad Palm KD0UWZ
Chaska, MN
KD0UWZ at scottares.org




# New MN SEC

## Section Emergency Manager Change

Joe Reinemann, KCØJCR, has been named as the new MN Section Emergency Manager by Skip Jackson , KSØJ, MN Section Manager.

Joe is an active amateur radio operator and dedicated public service volunteer with training and experience in emergency preparedness, disaster response and emergency communications.

He has led MN ARES in full scale exercises with the American Red Cross and Communications Exercises with MARS. He is a strong proponent of NBEMS and digital modes for emergency communications and is a regular participant of VHF and HF ARES nets.

Joe has volunteered his time, communications skills, and equipment in support for upwards of 25 public service events, including ultra-marathons, marathons, parades and bike rides. He is active both as a spotter and net control operator for Mankato Skywarn.

Previously, Joe has served ARRL as an Assistant District Emergency Coordinator, South Central Minnesota District Emergency Coordinator and Assistant Section Emergency Coordinator - Operations. Joe is currently living in rural St. Peter with his wife of 26 years.

Current MN SEM, Dan Anderson, KD0ASX, will continue to support Joe by serving MN ARES in a consulting capacity. The Section Emergency Manager transition will be completed by June 30, 2016.

Dan felt that the organization needed refreshing with new management. Dan consulted with Skip Jackson, MN SM, on the transition in MN ARES leadership. As part of the leadership transition Dan has provided Joe with training that will allow him to be an able successor in the SEC position.

Skip explained, " We have had the good fortune of having the services of Dan Anderson, KDØASX, Section Emergency Manager since July of 2009. Dan brought with him many years of experience in emergency management and a high level of skills in staff selection, training and motivation."

He said, "That Dan's experience and skill, combined with his focus and high energy has produced a high quality ARES organization in very good condition. We have now more than 50 counties (out of 87) with active ARES organizations, 7 districts with active District Emergency Managers and an excellent emergency response plan. Dan and his staff of volunteers have developed good relationships with served agencies in both government and private sectors."

You can keep up to date on ARES activity in the state on the MN ARES website located at: http://www.minnesotaares.org/ares/

*BREAK - OVER*

# Amateur Radio License Exam

Want to become a ham? Want to upgrade your license? You can find information and resources to success in ham radio at this page: http://www.scottares.org/License Info.htm
If you want to ask questions or find a local Elmer (Mentor) just drop an email to: newhaminfo@scottares.org

The hams in Scott ARES gather for breakfast the first Saturday of the month at the Perkins Restaurant in Savage. Bring you ham radio questions and talk to local amateur radio operators.

Now that you have done the work to study for your upgrade, here is where to find a convenient exam session near you. There is a VE exam search engine at: http://www.arrl.org/exam_sessions/search

Walk-ins allowed at most sessions however it is always best to check the details at the specific session you are planning to attend. Below is a list of scheduled sessions close to Scott County.
Good Luck!

**June 21, 2016** Monday 6:00 PM
SMARTS
Dale A. Blomgren (952) 402-2155
Email: kd0b@arrl.net
Location: Carver County Library
7711 Kerber Blvd
Chanhassen MN 55317
Walk-ins allowed, Pre-reg requested

**June 25, 2016** Saturday 9:00 AM
Sponsor: Bloomington Off/Emergency Mgmt
Daniel J. Royer (952) 888-9756
Email: dan-arrl@droyer.org
Location: City Hall-Police Department
1800 W Old Shakopee Rd
Bloomington MN 55431
Walk-ins allowed, Pre-reg requested

**July 13, 2016** Wednesday 7:00 PM
Sponsor: VARC
James C. Rice (612) 384-7709
Email: jrice@danpatch.org
Location: Perkins Restaurant & Bakery
17387 Kenyon Avenue
Lakeville MN 55044-4459
Walk-ins allowed, Pre-reg requested

**July 16, 2016** Saturday 9:00AM
Sponsor: SEMARC
Daniel M. Franz (651) 769-0358
Email: wd0gup@hotmail.com
Location: Zion Lutheran church
8500 Hillside Trl S
Cottage Grove MN 55016-3273

# Take a Dip in the General Pool

Time to test your knowledge of the information covered by the General Class license exam. Each month we'll take a look at a selection from the question pool.

Strap on your thinking cap and see what you can recall. Here is this month's sample:

1. What is the effect on an audio device or telephone system if there is interference from a nearby CW transmitter?
A. On-and-off humming or clicking
B. A CW signal at a nearly pure audio frequency
C. A chirpy CW signal
D. Severely distorted audio

2. What might be the problem if you receive an RF burn when touching your equipment while transmitting on an HF band, assuming the equipment is connected to a ground rod?
A. Flat braid rather than round wire has been used for the ground wire
B. Insulated wire has been used for the ground wire
C. The ground rod is resonant
D. The ground wire has high impedance on that frequency

3. What could be a symptom of a ground loop somewhere in your station?
A. You receive reports of "hum" on your station's transmitted signal
B. The SWR reading for one or more antennas is suddenly very high
C. An item of station equipment starts to draw excessive amounts of current
D. You receive reports of harmonic interference from your station

*(Check next month's issue of the ARES Communicator for the answer.)*

# May General Pool Answers

1. What signals are used to conduct a two-tone test?
B. Two non-harmonically related audio signals

2. Which of the following must be connected to an antenna analyzer when it is being used for SWR measurements?
C. Antenna and feed line

3. Which of the following can be determined with a field strength meter?
B. The radiation pattern of an antenna



BREAK - OVER

# SKYWARN => Directed Net Operation!

SKYWARN net managers recently distributed a recap of the operating procedures for use on a SKYWARN net. Participation in a spotter net is serious emergency communications. Everyone needs to remember that Rule # 1 is The net control station is in charge!

When severe weather conditions are rapidly developing across the metro area, time is at a premium. Do Not waste time with sloppy procedures and mindless chatter.

Think before you speak! Review the list of reportable conditions or print the information and keep it with your radio. No, really. You WILL screw it up when you are excited or rushed.

Really, think about what you are going to say BEFORE you hit the PTT switch. You can always tell when an operator is excited and rambles wasting time and lowering the professionalism of the net.

Please remember that Metro Skywarn Nets are "Controlled (Directed) Nets". You request access to the net with your MSW ID and a one word descriptors. Read and practice the following examples:.

1. Access the net with your Skywarn ID number, and a brief (one or two word) description of the reportable condition. ex: " 1119, hail, OVER" or " 1119 , wind damage, OVER or "1119, checkin, OVER." Wait for the net control to acknowledge your checck-in.

2. When Net operator acknowledges with your ID number, for example; " 1119" or " 1119, go ahead", give a brief and complete report that ends with your call sign. ex: "I'm located at I - 35W and I - 694. Pea - sized hail is covering the ground. Some the size of a dime. N0XXX, OVER "

3. One of two things will happen next: The Net Control operator may ask you questions to clarify your report. End each reply with your Amateur Radio callsign, OVER . OR The Net Control Operator will respond with time in 24 - hour format. This means your report has been received and understood, and that the Net is available for reports from other spotters . ex: "1732" This reporting format is intended to reduce the "on air" time for each report. Use of your callsign is required to be legal with the FCC.

You will find information to review at the following links:
https://metroskywarn.org/spotter-resources/spotter-reporting-guide
https://metroskywarn.org/front-page/47-board-communications/80-reminder-on-proper-spotter-reports

*BREAK - OVER*

# An Attack On The Grid?

## Power execs push back on Koppel claims

Eight months after veteran broadcast journalist Ted Koppel published a book predicting a devastating cyberattack on the U.S. power grid, leaders of the utility industry are sounding off over what they say is an exaggerated claim.

"We're speaking out on it now because we think there is an important story to tell," Scott Aaronson, the managing director for cyber and infrastructure security at the Edison Electric Institute, said last week at a briefing for reporters.
"If it's only going to be the movie-script scenarios, then I can understand why customers might lose confidence."

What Aaronson and others in the utility industry are taking issue with is a warning by Koppel in his bestselling book, *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*.

According to Koppel, who anchored the ABC news program *Nightline* from 1980 to 2005, the U.S. is likely to eventually suffer a cyberattack on its grid that could leave millions of Americans in the dark, short of water and food, and generally desperate for months.

The risk is considerable, Koppel claims, because the U.S. government and the utility industry are ill prepared to fend off such an assault by foreign adversaries and to help the nation recover from it.

Not so, Aaronson told reporters. "Part of what we want to do is interject a little bit of sanity and engineering and thoughtfulness into what can quickly devolve into a bit of a hysterical discussion," he said at the Washington headquarters of EEI, the trade association for investor-owned electric utilities.

As he did at recent House and Senate hearings on cybersecurity, Aaronson ticked off a number of steps taken by utilities and the government to address the threat, including standards requiring stepped-up protective measures and carrying penalties of up to $1 million per violation per day.

Moreover, utilities are increasingly coordinating to share information and expertise and to test their preparedness, including a drill conducted last fall by the industry's North American Electric Reliability Corporation, in which 4,400 participants from the industry and governments in the U.S., Canada and Mexico simulated coordinated cyber and physical attacks on the grid.

In the event of an incursion that disables electric infrastructure, power providers are expanding programs to share transformers and other equipment, and replace damaged equipment relatively quickly, Aaronson said.
"I disagree with the premise that we would be in a situation where we would have to deal with a months-long outage that would require people to shelter in place," he said.

As a sign of that resiliency, Aaronson recalled an attack on Pacific Gas & Electric's Metcalf substation south of San

**Grid Attacks** *cont'd on page 5*

# Test Your NIMS Knowledge

This month we continue our review of ICS-800: National Response Framework. The purpose of the National Response Framework is to ensure that all response partners across the Nation understand domestic incident response roles, responsibilities, and relationships in order to respond more effectively to any type of incident. The Framework focuses on response and short-term recovery instead of all of the phases of incident management.

Check your recall of the course material with this question.

1. The National Response Framework presents the guiding principles that:

A. Improve homeland security agencies' response to catastrophic natural hazards and terrorist-related incidents.

B. Update and supersede the National Incident Management System's framework based on lessons learned.

C. Enable all response partners to prepare for and provide a unified national response to all incidents.

D. Provide local, tribal, State, and Federal responders with specific operational plans for managing a wide range of incidents.

*Check next month's ARES Communicator for the solution*

# May NIMS Knowledge Solution

1. The National Preparedness Vision, National Planning Scenarios, Universal Task List, and Target Capabilities List are the four critical elements comprising the _____.

B. National Preparedness Guidelines

*BREAK - OVER*

# NBEMS Current Versions

The current version of the Fldigi manual is availale at NBEMS Info page at www.scottares.org. Look under the 'Help Sheets' heading.

Now is a good time to check to your digital software to make sure you are running the newest versions. You can find the most recent versions posted at both: www.w1hkj.com/download.html and http://www.scottares.org/NBEMS.htm

Here are the most recent releases as of June 15, 2016.

| Software | Version |
|---|---|
| Fldigi | 3.23.11 |
| Flwrap | 1.3.4 |
| Flmsg | 3.00.00 |
| Flamp | 2.2.03 |


The Monday evening training net is a great place to have your digi questions answered and problems solved! Join the Scott ARES group on 146.535 mHz simplex at 7:00pm on Monday evenings.

# Grid Attacks *- cont'd from page 4*

Jose in 2013 by unidentified snipers. The attack left 17 of the facility's 21 transformers destroyed and caused $15 million in damage.

"The lights didn't even blink in San Francisco and Silicon Valley," he said, adding that the substation was back in service in just over a month.

Nevertheless, Koppel remains unpersuaded by the industry's criticism of his book. "It is surely only a matter of time before a terrorist group, unrestrained by any geopolitical interests, acquires the capability to attack one of our power grids," he testified at a May hearing in the Senate where Aaronson also appeared.

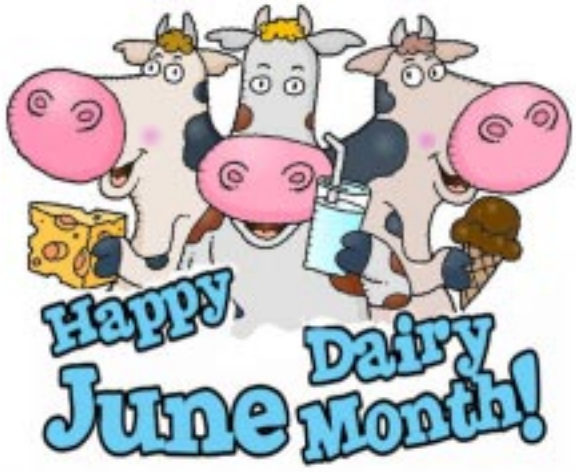
There's no dispute in the industry or the government that hackers want to disrupt power supplies and cause havoc in the U.S. In fact, the National Security Agency has acknowledged that "cyber intrusions" on control systems for the grid have increased, though none has caused a blackout.

But what Aaronson and his colleagues in the utility sector are trying to convey more now than before is that while there will always be room for improvement in addressing the risk, it isn't going unattended.

"You've got to be a little sensitive about how much you talk about it publicly," said Philip Moeller, EEI's senior vice president of energy delivery and a former member of theFederal Energy Regulatory Commission, who joined Aaronson at the press briefing.

"Particularly in the aftermath of Metcalf, we didn't want copycat attacks, which are much more likely to happen once it's in the headlines. But just because we don't talk about it doesn't mean a lot isn't being done."

*BREAK - OVER*



# Smarter Social Network Use

## Ten areas to protect yourself

Keep these ten topics in mind when you enter your personal information on social networks. You can lower your exposure to risky actions by being more thoughtful in your posting.

1. Your Full Birthdate - While you may love getting loads of birthday wishes posted by your friends on your Facebook Timeline, having your birthdate posted on your profile may provide scammers and identity thieves with one of the key pieces of information needed to steal your identity and open up accounts in your name.

2. Your Current Location - Many people don't realize that when they post a status update or a tweet, they may also be revealing their current location. Giving out your location information can be dangerous because it tells potential thieves that you might not be at home. Depending on your privacy settings, that innocent tweet from your vacation spot might give the bad guys the green light they were waiting for to rob your house.

3. Pictures of Your Children or Your Friends' Children Tagged With Their Names - Ok, this is a sensitive topic. We all want to protect our kids, we would lay down in front of a truck to protect them, but many of us post hundreds of name tagged pictures of our children online for the world to see. The problem is that you can never be sure that only your friends are seeing these pictures. What if your friend has their phone stolen or logs into Facebook from the library and forgets to log out? You can't rely on the "Friends only" setting because you really never know. Assume that everything is public and don't post anything that you wouldn't want the world having access to.

If you must post pictures of your children, remove any geotag information, and avoid using their real names in the picture tag or description.

4. Your Home Address - Again, you never know who might be looking at your profile. Don't post where you live as you are making things easy for the bad guys.

5. Your Real Phone Number - While you may want your friends to be able to contact you, what if your real phone number falls into the wrong hands. It's possible that your location could be narrowed down by someone using a reverse phone number lookup tool which are freely available on the Internet.

An easy way to allow people to contact you by phone without giving them your real phone number is by using a Google Voice phone number as a go-between.

6. Your Relationship Status - Want to give your stalker the green light they've been waiting for while simultaneously letting them know that your more likely to be home alone? Posting your relationship status is the surest way to accomplish this. If you want to be mysterious, just say "It's Complicated".

7. Pictures With Geotags - There's no better road map to your current location than a geotagged picture. Your phone might be recording the location of all pictures you take without you even knowing it. Find out about why geotags aren't necessarily as cool as you thought they were and to learn how to nix them from your pix. Search for information about "removing geotags".

8. Vacation Plans - "Hey, I'm going to be on vacation on the 25th of August, please come rob me", that's basically what you're saying to social network trolling criminals when you post your vacation plans, vacation photos, and when you location tag yourself while you're still on vacation. Wait until you are safely home before uploading your vacation pics or talking about your vacation online. Is "checking in" at that fancy restaurant really worth giving up your location information to potential criminals?

9. Embarrassing Things you Wouldn't Want Shared With Your Employer or Family - Before you post anything online, think to yourself, would I want my boss or family to see this? If not, don't post it. Even if you post something and delete it, doesn't mean that someone didn't take a screenshot of it before you had the chance to remove it.

10. Information About Your Current Job or Work-related Projects - Talking about work-related things on social networks is a bad idea. Even an innocent status update about how mad you are about missing a deadline on a project could provide valuable information to your competitors that they could leverage against your company.

Some companies have security awareness training. Check with your company to see if they have a security awareness training program to help educate employees about threats such as these.

*BREAK - OVER*

## Deep Thoughts

# Hacking!

It's in the news almost every day

So, what's the big deal about hacking and how can we protect ourselves?

Hackers use three common methods to acquire people's computer passwords: Brute Force , Social Engineering, and Administrator Back Doors. Knowing more about these techniques alps make sense of some password requirements and helps raise your surfing awareness.

**1) Brute Force** (aka 'Dictionary' Attacks) The term "brute force" means to overpower the defense through repetition. In the case of password hacking, brute forcing involves dictionary software that recombines English dictionary words with thousands of varying combination.
(Yes, much like a Hollywood safecracker movie scene, but much slower and much less glamorous). Brute force dictionaries always start with simple letters "a", "aa", "aaa", and then eventually moves to full words like "dog", "doggie", "doggy". These brute force dictionaries can make up to 50 attempts per minute in some cases.
Given several hours or days, these dictionary tools will overcome any password. The secret is to make it take days to crack your password.

**2) Social Engineering Attacks** Social engineering is the modern con game: the hacker manipulates you to divulge your password by using some kind of convincing personal contact. This personal contact might involve direct face-to-face communications, like a pretty girl with a clipboard doing interviews in a shopping mall. Social engineering attacks might also occur over the phone, where a hacker will masquerade as a bank representative calling to confirm your phone number and bank account numbers. The third and most common social engineering attack is called phishing or whaling.
Phishing and whaling attacks are deception pages masquerading as legitimate authorities on your computer screen. Phishing/ whaling emails will often redirect the victim to a convincing phishing website, where the victim types in their password, believing the website to be their actual bank or online account.

**3) Administrator Back Doors** This kind of attack is akin to stealing the building master keys from the building janitor: the perpetrator accesses the system as if they were an entrusted employee. In the case of computer administrators: special all-access accounts allow the user into areas where only trusted network administrator should go. These administrator areas include password recovery options. If the hacker can enter your system with the administrator's account, the hacker can retrieve passwords of most anyone on that system.

*BREAK - OVER*

# Having a Bad Day?

When you have an 'I hate My Job day' , even if you're retired, you sometimes have those days, try this out: On your way home from work, stop at your pharmacy and go to the thermometer section and purchase a rectal thermometer made by Johnson & Johnson.

Be very sure you get this brand. When you get home, lock your doors, draw the curtains and disconnect the phone so you will not be disturbed.

Change into very comfortable clothing and sit in your favorite chair. Open the package and remove the thermometer. Now, carefully place it on a table or a surface so that it will not become chipped or broken.

Now the fun part begins.

Take out the literature from the box and read it carefully. You will notice that in small print there is a statement:

"Every Rectal Thermometer made by Johnson & Johnson is personally tested and then sanitized."

Now, close your eyes and repeat out loud five times,' I am so glad I do not work in the thermometer quality control department at Johnson & Johnson.'

Have a nice day; and remember, there is always someone else with a job that is more of a pain in the ass than yours!

**ARES Breakfast**
Saturday July 9th
7:30AM
Perkins Restaurant
Savage, MN

# NECOS Schedule June 2016

The first Monday or the month the net is held on the WB0RMK repeater, Carver. You will find WB0RMK here: 147.165/765 PL 107.2

| | |
|---|---|
| June 20 | KD0UWZ Chad |
| June 27 | KB0FH Bob |
| **July 2014** | |
| July 4 | N0BHC Bob |
| July 11 | WA0DGW John |
| July 18 | KD0UWZ Chad |
| July 25 | KB0FH Bob |
| Aug 1 | KD0UWZ Chad |